

```

<HTML><HEAD>
<META HTTP-EQUIV="Content-type" CONTENT="text/html; charset=x-sjis">
<!-- <META HTTP-EQUIV="Pragma" CONTENT="no-cache"> -->
<TITLE>Searching PAJ</TITLE>
</HEAD>

<BODY BGCOLOR="#FFFFFF" TEXT="#000000" LINK="#000066" VLINK="#808080"
ALINK="#FF0000" TOPMARGIN="0">
<BR><CENTER><H2><B>PATENT ABSTRACTS OF JAPAN</B></H2></CENTER>

<TABLE BORDER="0" WIDTH="100%">
<TR><TD WIDTH="40%" VALIGN="top"><BR></TD>
<TD WIDTH="15%" NOWRAP>(11)</TD><TD VALIGN="top">
<TD WIDTH="45%"><B>2002-091827</B></TD></TR>
<TR><TD WIDTH="40%" VALIGN="top"><BR></TD>
<TD WIDTH="15%" NOWRAP>(43)</TD><TD VALIGN="top">
<TD WIDTH="45%"><B>29.03.2002</B></TD></TR>
</TABLE>
<HR WIDTH="100%" SIZE="5">

<TABLE BORDER="0" WIDTH="100%">
<TR>
<TD VALIGN="top" WIDTH="40%">(51)Int.Cl.</TD>
<TD VALIGN="top" WIDTH="60%"><PRE><B> G06F 12/14
</B><BR><B> G06F 12/00
</B><BR><B> G06F 17/60
</B><BR></PRE></TD>
</TR>
</TABLE>
<HR WIDTH="100%" SIZE="5">

<TABLE BORDER="0" WIDTH="100%">
<TR>
<TD WIDTH="15%" NOWRAP VALIGN="top">(21)</TD><TD><TD WIDTH="25%" VALIGN="top"><B>2000-284862</B></TD>
<TD WIDTH="15%" NOWRAP VALIGN="top">(71)</TD><TD WIDTH="45%" VALIGN="top"><B>SANYO ELECTRIC CO LTD</B></TD>
</TR>
<TR>
<TD WIDTH="15%" NOWRAP VALIGN="top">(22)</TD><TD WIDTH="25%" VALIGN="top"><B>20.09.2000</B></TD>
<TD WIDTH="15%" NOWRAP VALIGN="top">(72)</TD><TD WIDTH="45%" VALIGN="top"><B>HORI YOSHIHIRO</B></TD>
</TR>
</TABLE>
<HR WIDTH="100%" SIZE="5">

<!-- __PRIORITY_DELETE__
<TABLE BORDER="0">
<TR><TD>(30)</TD></TR>
<TR>
<TD VALIGN="top"><B>Priority number :</B></TD>
<TD VALIGN="top"><B>Priority date :</B></TD>
<TD VALIGN="top"><B>Priority country :</B></TD>
</TR>
</TABLE>
<HR WIDTH="100%" SIZE="5">
__PRIORITY_DELETE__-->

<TABLE BORDER="0" WIDTH="100%">

```

<TR><TD>(54)<B> DATA TERMINAL EQUIPMENT<BR></B></TD></TR>  
 <TR><TD VALIGN="top">

&nbsp;

(57)Abstract:<BR>  
 PROBLEM TO BE SOLVED: To provide portable terminal equipment for receiving only required enciphered contents data and/or license key or the like from a distribution server.<BR>  
 SOLUTION: When the receiving request of enciphered contents data {Data}Kc is inputted from a user, a portable telephone set retrieves the recording conditions of a contents ID, license key Kc, reproducing time limit information AC1, reproducing time limit and enciphered contents data {Data}Kc or the like on a loaded memory card. Then, only the enciphered contents data {Data}Kc and license (contents ID, license key Kc, reproducing time limit information AC1 and reproducing time limit), which are not recorded in a license area 1415A and a data area 1415B of the memory card are received from the distribution server.<BR><BR>  
 </TD></TR>  
 </TABLE>

<HR WIDTH="100%" SIZE="5">

#### LEGAL STATUS

<TABLE BORDER="0" WIDTH="100%">  
 <TR><TD WIDTH="50%">[Date of request for examination]</TD>  
   <TD WIDTH="50%" VALIGN="top" ALIGN="left"></TD>  
 </TR>  
 <TR><TD WIDTH="50%" VALIGN="top">[Date of sending the examiner's decision of rejection]</TD>  
   <TD WIDTH="50%" VALIGN="top" ALIGN="left"></TD>  
 </TR>  
 <TR><TD WIDTH="50%" VALIGN="top">[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]</TD>  
   <TD WIDTH="50%" VALIGN="top" ALIGN="left"></TD>  
 </TR>  
 <TR><TD WIDTH="50%" VALIGN="top">[Date of final disposal for application]</TD>  
   <TD WIDTH="50%" VALIGN="top" ALIGN="left"></TD>  
 </TR>  
 <TR><TD WIDTH="50%" VALIGN="top">[Patent number]</TD>  
   <TD WIDTH="50%" VALIGN="top" ALIGN="left"></TD>  
 </TR>  
 <TR><TD WIDTH="50%" VALIGN="top">[Date of registration]</TD>  
   <TD WIDTH="50%" VALIGN="top" ALIGN="left"></TD>  
 </TR>  
 <TR><TD WIDTH="50%" VALIGN="top">[Number of appeal against examiner's decision of rejection]</TD>  
   <TD WIDTH="50%" VALIGN="top" ALIGN="left"></TD>  
 </TR>  
 <TR><TD WIDTH="50%" VALIGN="top">[Date of requesting appeal against examiner's decision of rejection]</TD>  
   <TD WIDTH="50%" VALIGN="top" ALIGN="left"></TD>  
 </TR>  
 <TR><TD WIDTH="50%" VALIGN="top">[Date of extinction of right]</TD>  
   <TD WIDTH="50%" VALIGN="top" ALIGN="left"></TD>  
 </TR>  
 </TABLE>

<!--\_\_CORRECT\_DELETE\_\_>  
 <HR WIDTH="100%" SIZE="5">  
 CORRECTION<BR>  
 <TABLE BORDER="0">  
   \_\_CORRECT\_DATA\_\_  
 </TABLE>  
 \_\_CORRECT\_DELETE\_\_-->

<BR><BR><HR>CLAIMS  
<HR>[Claim(s)]

<BR>[Claim 1]

The license for reproducing the encryption contents data which enciphered contents data, and/or said encryption contents data is received from a distribution server. The data-logging section which is the Data Terminal Equipment which records said encryption contents data and/or said license, and records said encryption contents data and said license,  
It has the interface which controls data transfer with the transceiver section which performs the communication link with the exterior, and said data-logging section, the key stroke section for inputting directions, and a control section. Said control section  
If the request to receipt of encryption contents data is inputted through said key stroke section  
It searches whether the encryption contents data by which request to receipt was carried out are recorded on said data recorder.  
And when the existence of the license which can reproduce the encryption contents data by which request to receipt was carried out is searched and said encryption contents data are not recorded on said data-logging section,  
And/or, the Data Terminal Equipment which requires distribution of said encryption contents data and/or said license of a distribution server through said transceiver section when said license cannot be found.  
<BR>[Claim 2]

Said control section is a Data Terminal Equipment according to claim 1 which performs retrieval of said encryption contents data and/or said license after the encryption contents data said transceiver section carries out [ data ] request to receipt based on the menu information on the encryption contents data received from said distribution server are determined.  
<BR>[Claim 3]

It is the Data Terminal Equipment according to claim 2 with which said decision of encryption contents data which carries out request to receipt is made by choosing the content ID for specifying the encryption contents data contained in said menu information, and said control section performs retrieval of said encryption contents data and/or said license based on said selected content ID.  
<BR>[Claim 4]

Said control section is a Data Terminal Equipment given in any 1 term of claim 1 to claim 3 which requires distribution of said encryption contents data of said distribution server through said transceiver section when said encryption contents data are searched and said encryption contents data are not recorded on said data-logging section.  
<BR>[Claim 5]

Said control section is a Data Terminal Equipment according to claim 4 with which said license is searched when said encryption contents data are recorded on said data recorder.  
<BR>[Claim 6]

It is the Data Terminal Equipment according to claim 1 which said license consists of the license key for decoding said encryption contents data at least, and the playback limit information that playback of said encryption contents data is restricted, and judges that said license cannot be found when the encryption contents data with which request to receipt of said control section was carried out are recorded on said data-logging section and said license key and said playback limit information are not recorded on said data-logging section.  
<BR>[Claim 7]

A license key for said license to decode said encryption contents data at least,  
Page 3

It consists of the playback limit information that playback of said encryption contents data is restricted. Said control section

The license key for decoding the encryption contents data by which request to receipt was carried out, and its encryption contents data is recorded on said data-logging section.  
The Data Terminal Equipment according to claim 1 judged that said license cannot be found when playback of said encryption contents data is restricted by said playback limit information.

<BR>[Claim 8]

Said control section is a Data Terminal Equipment according to claim 7 which transmits the playback limit information after modification inputted from said key stroke section to said distribution server through said transceiver section with said content ID as purchase conditions for said license.

<BR>[Claim 9]

It is the Data Terminal Equipment according to claim 3 which acquires said content ID by having a display further by inputting the information for choosing said content ID based on said menu information as which said control section displayed said menu information on said display, and the user was displayed on said display through the key stroke section.

<BR>[Claim 10]

Said control section is a Data Terminal Equipment according to claim 9 which said menu information consists of two or more screens including the shift information for shifting to other screens, and will display other screens determined based on said shift information on said display if said shift information is inputted from said input section including the input section for said display to input said shift information.

<BR>[Claim 11]

Said control section is a Data Terminal Equipment given in any 1 term of claim 1 to claim 10 which receives said license only when the purchase conditions of said license, and the authentication data and said content ID of said data-logging section acquired through said interface are transmitted to said distribution server through said transceiver section and said authentication data are attested in said distribution server.

<BR>[Claim 12]

It has further the data playback section which reproduces said encryption contents data according to said license. Said control section

If the playback demand of encryption contents data is inputted through said key stroke section

Said interface is minded for information required for said data playback section at least, and said encryption contents data from said data-logging section among said licenses over said encryption contents data. A receipt,

A Data Terminal Equipment given in any 1 term of claim 1 to claim 11 which gives the received encryption contents data and said required information to said data playback section.

<BR>[Claim 13]

It connects with said bus and has further the authentication data-hold section holding the authentication data to said data-logging section. At the time of playback of encryption contents data said control section

Only when said authentication data are attested in said data-logging section, said interface is minded for information required for said data playback section at least from said data-logging section among said licenses over said encryption contents data. A receipt,

The Data Terminal Equipment according to claim 12 which gives the received encryption contents data and said required information to said data playback section.

<BR>[Claim 14]

Said data-logging section is a Data Terminal Equipment given in any 1 term of claim 1 to claim 13 which is a removable data recorder.

<BR><BR>

<BR><BR><HR>DETAILED DESCRIPTION

<HR>[Detailed Description of the Invention]

<BR>[0001]

<BR>[Field of the Invention]

This invention relates to the Data Terminal Equipment used in the data distribution system which makes possible the protection of copyrights to the copied information.  
<BR>[0002]

<BR>[Description of the Prior Art]

Each user is able to access network information easily in recent years with the terminal for the individuals [ advance / of information communication networks, such as the Internet, etc. ] using a portable telephone etc.

<BR>[0003]

In such an information communication network, information is transmitted by the digital signal.

It is possible to perform a copy of data, without producing most degradation of the tone quality by such copy, or image quality, even when an individual user copies the music and image data which followed, for example, were transmitted in the above information communication networks.

<BR>[0004]

Therefore, if the policy for suitable protection of copyrights is not taken when the creation object with which the access of authors, such as music data and image data, exists on such an information communication network is transmitted, there is a possibility of infringing on a copyright person's access remarkably.

<BR>[0005]

On the other hand, top priority is given to the object of protection of copyrights, and supposing it cannot distribute work data through the digital information communication network which carries out sudden expansion size, it will become rather disadvantageous also for the copyright person who can collect a fixed royalty on the occasion of the duplicate of work data fundamentally.

<BR>[0006]

Here, about CD (compact disk) which recorded the music data usually sold, if it thinks and sees not taking the case of distribution through the above digital information communication networks but taking the case of the record medium which recorded the digital data, the music copy of data from CD to magneto-optic disks (MD etc.) can be freely performed in principle, as long as the copied music concerned is stopped to an individual activity.

However, the individual user who performs digital sound recording etc. is to pay indirectly the fixed amount of the prices of media, such as the digital sound recorder machine itself and MD, as a deposit to a copyright person.

<BR>[0007]

And in view of such information being digital data which do not almost have copy degradation, when the music data which are a digital signal are copied to MD from CD, for protection of copyrights, copying music information to MD of further others as digital data from recordable MD could not do a device constitutionally, and it is come.

<BR>[0008]

Since distributing music data and image data to the public through a digital information communication network also from such a situation is an act from which itself receives the limit by a copyright person's public transmission right,

sufficient policy for protection of copyrights needs to be devised.  
<BR>[0009]

In this case, it is necessary for the contents data received once to prevent being reproduced still more freely about contents data which are the works transmitted to the public through an information communication network, such as music data and image data.  
<BR>[0010]

Then, the data distribution system by which the distribution server holding the encryption contents data which enciphered contents data distributes encryption contents data through a terminal unit to the memory card with which terminal units, such as a portable telephone, were equipped is proposed.  
In this data distribution system, it transmits to a distribution server in the case of the distribution demand of the open cryptographic key and certificate of the memory card beforehand attested by the certificate authority of encryption contents data, and the license key for decoding encryption contents data and encryption contents data to a memory card, after checking having received the certificate with which the distribution server was attested is transmitted.  
And in case encryption contents data and a license key are distributed, a distribution server and a memory card generate a different session key for every distribution, by the generated session key, encipher a open cryptographic key and exchange keys a distribution server and between memory cards.  
<BR>[0011]

Eventually, a distribution server transmits the license which it was enciphered by the open cryptographic key of memory card each, and was further enciphered by the session key, and encryption contents data to a memory card.  
And a memory card records the license key and encryption contents data which were received on a memory card.  
<BR>[0012]

And a cellular phone is equipped with a memory card when reproducing the encryption contents data recorded on the memory card.  
A cellular phone also has a specialized circuit for decoding the encryption contents data from a memory card other than the usual telephone function, and reproducing, and outputting to the exterior.  
<BR>[0013]

Thus, the user of a portable telephone can receive encryption contents data from a distribution server using a portable telephone, and can reproduce the encryption contents data.  
<BR>[0014]

<BR>[Problem(s) to be Solved by the Invention]

However, when receiving encryption contents data from a distribution server, a portable telephone receives the purchase conditions which set up the count of playback of the license key which decodes encryption contents data with encryption contents data, and encryption contents data, playback length, etc. from a distribution server, and records them on a memory card.  
<BR>[0015]

Moreover, a portable telephone reproduces encryption contents data, when not restricted by a count of playback, playback length, etc. which playback of encryption contents data received when reproducing encryption contents data.  
<BR>[0016]

Furthermore, a portable telephone may receive only encryption contents data from other than a distribution server, and may record them on a memory card.  
<BR>[0017]

Therefore, although encryption contents data are recorded on the memory card, when  
Page 6

the license key is not recorded on a memory card, encryption contents data and a license key are recorded on the memory card, but when playback of encryption contents data is restricted by the count of playback, playback length, etc., the case where encryption contents data and a license key are not recorded on a memory card etc. is assumed.  
<BR>[0018]

having required distribution of encryption contents data, a license key, etc. of the distribution server promptly, when the distribution demand of encryption contents data was carried out from a user in this case -- if -- the same encryption contents data and a license key are received from a distribution server -- \*\*\*\*\* -- the same encryption contents data -- receiving -- a tariff -- multiple-times payment -- it may be unacquainted and a problem arises.  
<BR>[0019]

Moreover, in order to receive encryption contents data from a distribution server, there is also a problem of needing unnecessary time amount.  
<BR>[0020]

Then, it is made in order that this invention may solve this problem, and the object is offering the Data Terminal Equipment which receives chisels, such as required encryption contents data and/or a license key, from a distribution server.  
<BR>[0021]

<BR>[The means for solving a technical problem and an effect of the invention]

The Data Terminal Equipment by this invention receives the license for reproducing the encryption contents data and/or encryption contents data which enciphered contents data from a distribution server.  
The data-logging section which is the Data Terminal Equipment which records encryption contents data and/or a license, and records encryption contents data and a license,  
It has the interface which controls data transfer with the transceiver section which performs the communication link with the exterior, and the data-logging section, the key stroke section for inputting directions, and a control section. A control section  
If the request to receipt of encryption contents data is inputted through the key stroke section  
It searches whether the encryption contents data by which request to receipt was carried out are recorded on the data-logging section.  
And when the existence of the license for reproducing the encryption contents data by which request to receipt was carried out is searched and encryption contents data are not recorded on the data-logging section,  
And/or, when there is no license, distribution of encryption contents data and/or a license is required of a distribution server through the transceiver section.  
<BR>[0022]

In the Data Terminal Equipment by this invention, if the request to receipt of encryption contents data is inputted through the key stroke section from a user, a control section will search whether the encryption contents data and/or the license with which request to receipt was made are recorded on the data-logging section, and will require distribution of the encryption contents data which are not recorded on the data-logging section, and/or a license of a distribution server.  
That is, a Data Terminal Equipment receives only required encryption contents data and a required license from a distribution server according to the encryption contents data in the data-logging section, and the record situation of a license, and records them on the data-logging section.  
<BR>[0023]

Therefore, according to this invention, the encryption contents data in the data-logging section and the duplicate record of a license can be prevented.  
<BR>[0024]

Moreover, according to this invention, it can prevent paying the useless tariff by overlapping and receiving a license to a distribution server.  
<BR>[0025]

Furthermore, according to this invention, it can prevent that useless time amount generates encryption contents data by overlapping and receiving.  
<BR>[0026]

Preferably, the control section of a Data Terminal Equipment performs retrieval of encryption contents data and/or a license, after the encryption contents data the transceiver section carries out [ data ] request to receipt based on the menu information on the encryption contents data received from the distribution server are determined.  
<BR>[0027]

A Data Terminal Equipment performs retrieval of encryption contents data and/or a license, after the encryption contents data which carry out request to receipt are determined based on the menu information received from the distribution server.  
<BR>[0028]

Therefore, according to this invention, it can judge to accuracy whether the encryption contents data and the license by which request to receipt was carried out are recorded on the data-logging section.  
<BR>[0029]

The decision of encryption contents data which carries out request to receipt is preferably made by choosing the content ID for specifying the encryption contents data contained in menu information, and a control section performs retrieval of encryption contents data and/or a license based on the selected content ID.  
<BR>[0030]

A user chooses the encryption contents data which carry out request to receipt by specifying the content ID of encryption contents data.  
If it does so, the control section of a Data Terminal Equipment will extract the content ID of selected encryption contents data, and will search whether encryption contents data and/or a license are recorded on the data-logging section based on the extracted content ID.  
<BR>[0031]

Therefore, according to this invention, retrieval of the encryption contents data in the data-logging section and/or a license can be performed to accuracy.  
<BR>[0032]

Preferably, the control section of a Data Terminal Equipment requires distribution of encryption contents data of a distribution server through the transceiver section, when encryption contents data are searched and encryption contents data are not recorded on the data-logging section.  
<BR>[0033]

The control section of a Data Terminal Equipment requires distribution of encryption contents data and a license of \*\*\*\* which searches the license in the data-logging section to a distribution server, when the encryption contents data in the data-logging section are searched using content ID and encryption contents data are not recorded on the data-logging section.  
<BR>[0034]

Therefore, according to this invention, the encryption contents data in the data-logging section and the record situation of a license are searched promptly, and required encryption contents data and a required license can be received from a distribution server according to that record situation.  
<BR>[0035]

Preferably, the control section of a Data Terminal Equipment searches a license,  
Page 8



when encryption contents data are recorded on the data-logging section.  
<BR>[0036]

The control section of a Data Terminal Equipment searches a license, after checking that encryption contents data are not recorded on the data-logging section.  
<BR>[0037]

Therefore, according to this invention, by performing only required retrieval, retrieval time can be shortened and exact retrieval can be performed.  
<BR>[0038]

Preferably, a license consists of the license key for decoding encryption contents data at least, and the playback limit information that playback of encryption contents data is restricted, and the encryption contents data by which request to receipt was carried out are recorded on the data recorder, and a control section judges that there is no license, when a license key and playback limit information are not recorded on the data-logging section.  
<BR>[0039]

when the license key and playback limit information which constitute a license are not recorded on the data-logging section, the control section of a Data Terminal Equipment judges that the license of encryption contents data by which request to receipt was carried out wants to exist.  
<BR>[0040]

Therefore, according to this invention, when only encryption contents data are recorded on the data-logging section, a license key and playback limit information can be received from a distribution server.  
<BR>[0041]

A license consists preferably of the license key for decoding encryption contents data at least, and the playback limit information restrict playback of encryption contents data, and it judges that there is [ control section ] nothing in a license when the license key for decoding the encryption contents data by which request to receipt was carried out, and its encryption contents data is recorded on the data-logging section and playback of encryption contents data is restricted by playback limit information.  
<BR>[0042]

when only the playback limit information which constitutes a license is not recorded on the data-logging section, the control section of a Data Terminal Equipment judges that the license of encryption contents data by which request to receipt was carried out does not exist.  
<BR>[0043]

Therefore, according to this invention, when only playback limit information is not recorded on the data-logging section, playback limit information can be received from a distribution server, and a license can be acquired.  
<BR>[0044]

Preferably, the control section of a Data Terminal Equipment transmits to a distribution server through the transceiver section with content ID as purchase conditions for a license of the playback limit information after modification inputted from the key stroke section.  
<BR>[0045]

The control section of a Data Terminal Equipment will transmit the purchase conditions set up with content ID to a distribution server, if the purchase conditions of encryption contents data are set up by changing only playback limit information.  
And a Data Terminal Equipment receives playback limit information from a distribution server, and records it on the data-logging section.  
<BR>[0046]

Therefore, according to this invention, also when a license is purchased, encryption contents data are reproduced and a license is lost, encryption contents data can be reproduced by newly purchasing only playback limit information from a distribution server.

<BR>[0047]

Preferably, content ID is acquired by equipping a Data Terminal Equipment with a display further, and inputting the information for choosing content ID based on the menu information as which the control section displayed menu information on the display, and the user was displayed on the display through the key stroke section.

<BR>[0048]

The menu information distributed from the distribution server is displayed on the display of a Data Terminal Equipment. And a user inputs the information for choosing the content ID of encryption contents data which looks at the menu information displayed on the display, and wishes to receive from the key stroke section.

If it does so, a control section will acquire the content ID chosen through the key stroke section.

<BR>[0049]

Therefore, according to this invention, a user can determine the encryption contents data which wish to receive based on vision information.

Moreover, since the information for choosing content ID is inputted according to this invention, a control section can perform retrieval of encryption contents data and/or a license promptly based on the selected content ID.

<BR>[0050]

Preferably, menu information consists of two or more screens including the shift information for shifting to other screens, and a control section will display other screens determined based on shift information on a display, if shift information is inputted from the input section including the input section for a display to input shift information.

<BR>[0051]

If a user inputs and does shift information so when the encryption contents data which wish to receive are not contained in the menu information displayed on the display of a Data Terminal Equipment, the control section of a Data Terminal Equipment will shift to the next screen, and will display new menu information on a display.

<BR>[0052]

Therefore, according to this invention, the encryption contents data which wish to receive can be chosen from many encryption contents data.

<BR>[0053]

Preferably, the control section of a Data Terminal Equipment receives a license, only when the purchase conditions of a license, and the authentication data and content ID of the data-logging section which were acquired through the interface are transmitted to a distribution server through the transceiver section and authentication data are attested in a distribution server.

<BR>[0054]

only when a distribution server attests the authentication data sent from the data-logging section, a Data Terminal Equipment receives a license.

<BR>[0055]

Therefore, according to this invention, it can license only to the regular data-logging section.

Consequently, protection of encryption contents data can be aimed at.

<BR>[0056]

A Data Terminal Equipment is preferably equipped further with the data playback section which reproduces encryption contents data according to a license, and a control section will give a receipt, its received encryption contents data, and required information through an interface to the data playback section from the data-logging section among the licenses over encryption contents data for information required for the data playback section at least, and encryption contents data, if the playback demand of encryption contents data is inputted through the key-stroke section.  
<BR>[0057]

A control section gives drawing, encryption contents data, and information required for playback to the data playback section from the data-logging section only for information required for playback among the various information which constitutes a license at the time of playback of encryption contents data.  
And the data playback section decodes and reproduces encryption contents data using required information.  
<BR>[0058]

Therefore, according to this invention, information required for playback can restrict playback of encryption contents data.  
<BR>[0059]

Preferably, a Data Terminal Equipment is further equipped with the authentication data-hold section holding the authentication data to the data-logging section, and at the time of playback of encryption contents data, a control section gives [ among the licenses over encryption contents data ] a receipt and its received encryption contents data to the data playback section through an interface from the data-logging section for information required for the data playback section at least, only when authentication data are attested in the data-logging section.  
<BR>[0060]

Only when reproducing the encryption contents data received from the distribution server and the justification of a Data Terminal Equipment to the data-logging section is checked, a Data Terminal Equipment reproduces a receipt and encryption contents data for encryption contents data from the data-logging section.  
<BR>[0061]

Therefore, according to this invention, only a regular Data Terminal Equipment can reproduce encryption contents data.  
Consequently, the illegal copy of encryption contents data etc. can be prevented and protection can be aimed at.  
<BR>[0062]

It is a data recorder with the data-logging section it is desirable and removable from a Data Terminal Equipment.  
<BR>[0063]

a Data Terminal Equipment will hold and record the encryption contents data and license which were received on a removable data recorder, if encryption contents data and a license are received from a distribution server.  
<BR>[0064]

Therefore, according to this invention, encryption contents data and/or a license are recordable on two or more data recorders.  
<BR>[0065]

<BR>[Embodiment of the Invention]

It explains to a detail, referring to a drawing about the gestalt of operation of this invention.  
In addition, the same sign is given to the same or a considerable part among drawing, and the explanation is not repeated.  
<BR>[0066]

<A  
 HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran\_web.cgi\_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FNO000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000003"  
 TARGET="tjitemdrw">Drawing 1</A>  
 is a schematic diagram for explaining notionally the whole data distribution system configuration which distributes the encryption contents data which the personal digital assistant equipment by this invention makes a reproductive object to a memory card.  
 <BR>[0067]

In addition, although explained taking the case of the data distribution structure of a system which distributes digital music data to each cellular-phone user through a portable telephone network below, this invention can be applied, without being limited in such a case, when distributing the contents data as other works, for example, image data, dynamic-image data, etc., so that it may become clear by the following explanation.  
 <BR>[0068]

with reference to

<A  
 HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran\_web.cgi\_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FNO000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000003"  
 TARGET="tjitemdrw">drawing 1</A>  
 , the distribution carrier 20 relays the distribution demand (distribution request) from each cellular-phone user who got through the cellular-phone network of self to a license server.  
 The license server 10 which manages the music data with which copyright exists [ whether the memory card 110 with which a cellular-phone user's portable telephone 100 accessed in quest of data distribution was equipped has just authentication data, and ]  
 Namely, after performing authentication processing of whether to be the memory card of normal and enciphering music data (it is also called contents data below) with a predetermined cipher system to a just memory card  
 It licenses as information required for the cellular phone company which is the distribution carrier 20 for distributing data in order to reproduce such encryption contents data and encryption contents data.  
 <BR>[0069]

The distribution carrier 20 distributes encryption contents data and a license through a cellular-phone network and a portable telephone 100 to the memory card 110 with which the portable telephone 100 which transmitted the distribution demand through the cellular-phone network of self was equipped.  
 <BR>[0070]

In

<A  
 HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran\_web.cgi\_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FNO000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000003"  
 TARGET="tjitemdrw">drawing 1</A>  
 , it has the composition that a cellular-phone user's portable telephone 100 is equipped with the removable memory card 110, for example.  
 A memory card 110 is given to the music playback section in a portable telephone 100 (not shown) after decoding the encryption performed in a receipt and the above-mentioned distribution in the encryption contents data received by the portable telephone 100.  
 <BR>[0071]

furthermore -- for example, the head telephone 130 grade which the cellular-phone user connected to the portable telephone 100 -- minding -- such contents data --  
 Page 12

&quot;-- reproducing, &quot; carrying out and hearing is possible.  
<BR>[0072]

Below, it will combine with such a license server 10 and the distribution carrier 20, and will be named the distribution server 30 generically.  
<BR>[0073]

Moreover, suppose that the processing which transmits contents data to each portable telephone etc. is called &quot;distribution&quot;; from such a distribution server 30.  
<BR>[0074]

It becomes a difficult configuration to play music in response to distribution of contents data first, by considering as such a configuration, from the distribution server 30, if a memory card 110 is not used.  
<BR>[0075]

And in the distribution carrier 20, it becomes easy that the distribution carrier 20 collects the royalty generated by carrying out counting of the frequency whenever it distributes the contents data for one music whenever a cellular-phone user receives contents data (download) with the phonecall charges of a portable telephone, then for a copyright person to secure a royalty.  
<BR>[0076]

Being needed on a system, in order to make refreshable the contents data enciphered and distributed in a configuration as shown in  
<A  
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran\_web.cgi\_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000003"  
TARGET="tjitemdrw">drawing 1</A>  
at the user side of a cellular phone  
It is a method for distributing the cryptographic key in a communication link to the 1st. Further to the 2nd  
It is the method itself which enciphers contents data to distribute, and is the configuration of realizing contents data protection for preventing further the unapproved copy of the contents data distributed to the 3rd in this way.  
<BR>[0077]

The recording apparatus and data playback terminal (the data playback terminal which can reproduce contents is also called portable telephone.) with which authentication and the check function of this invention of operation of as opposed to [ in / especially in a gestalt / the time of distribution and generating of each reproductive session ] the migration place of these contents data were enriched, and un-attesting or a decode key was torn  
the following -- being the same -- by preventing the output of the contents data to receive explains the configuration which strengthens the protection of copyrights of contents data.  
<BR>[0078]

<A  
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran\_web.cgi\_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000004"  
TARGET="tjitemdrw">Drawing 2</A>  
is drawing explaining properties, such as data for the communication link used, and information, in the data distribution system shown in  
<A  
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran\_web.cgi\_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000003"  
TARGET="tjitemdrw">drawing 1</A>

<BR>[0079]

First, the data distributed from the distribution server 30 are explained. Data(s) are contents data, such as music data. Encryption which can be decoded with the license key Kc is given to the contents data Data. Encryption contents {data Data} Kc to which encryption which can be decoded with the license key Kc was given is distributed to a cellular-phone user from the distribution server 30 in this format.  
<BR>[0080]

In addition, in the following, it shall be shown that a notation called {Y} X gave encryption which can be decoded with the decode key X for Data Y.  
<BR>[0081]

Furthermore, from the distribution server 30, additional information Data-inf as plaintext information, such as copyright about contents data or server access relation, is distributed with encryption contents data. Moreover, the transaction ID which is control code for specifying distribution of the encryption contents data from the distribution server 30, a license key, etc. is exchanged between the distribution server 30 and a portable telephone 100. Furthermore, the license ID which is control code which can specify issuance of the content ID which is a code for identifying the contents data Data as license information, and a license are generated based on the license purchase conditions AC including information determined by assignment from a user side, such as the number of licenses, and functional definition. The playback length AC2 grade which are the access-restriction information AC 1 which is the information about the limit to access of a recording device (memory card), and the control information in a data playback terminal exists. Henceforth, suppose that the license key Kc, content ID, License ID, the count length AC 1 of playback, and the playback length AC 2 are combined, and it is named a license generically.  
<BR>[0082]

<A  
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran\_web.cgi\_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000005"  
TARGET="tjitemdrw">Drawing 3c</A>  
is drawing explaining properties, such as data for employment of the authentication used in the data distribution system shown in  
<A  
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran\_web.cgi\_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000005"  
TARGET="tjitemdrw">drawing 1c</A>  
, and an inhibited class list, and information.  
<BR>[0083]

In the gestalt of operation of this invention, for every class of the portable telephone which reproduces a recording apparatus (memory card) and contents data, the inhibited class list CRL (Class Revocation List) is employed so that distribution of contents data and playback can be forbidden. Below, notation CRL may express the data in an inhibited class list if needed.  
<BR>[0084]

The inhibited class list data CRL which listed the class of the portable telephone with which distribution of a license and playback are forbidden, and a memory card are contained in inhibited class list related information.  
<BR>[0085]

while the inhibited class list data CRL are managed within the distribution server  
Page 14

30, record maintenance of them is carried out also into a memory card. Although it is necessary to upgrade at any time and to update data, about modification of data, such an inhibited class list judges the existence of renewal of the inhibited class list received from the portable telephone on the basis of the time at the time of distributing the license of encryption contents data, a license key, etc. fundamentally, and when not updated, it distributes the updated inhibited class list to a portable telephone. moreover, the difference which reflected only the changed part about modification of an inhibited class list -- \*\* considered as the configuration which generates data CRL\_dat from the distribution server 30 side, and by which the inhibited class list CRL of [ in a memory card ] is rewritten according to this is possible. Moreover, about the version of an inhibited class list, CRL\_ver is outputted from a memory card side and version control is performed by checking this by the distribution server 30 side. difference -- the information on a new version is also included in data CRL\_dat.  
<BR>[0086]

Thus, supply of the license key to the portable telephone and memory card by which the decode key of a proper was torn is forbidden to the class of a class proper, i.e., a portable telephone, and memory card by carrying out maintenance employment of the inhibited class list CRL not only a distribution server but into a memory card. It becomes impossible for this reason, for playback of contents data to move contents data in a portable telephone at a memory card.  
<BR>[0087]

Thus, the inhibited class list CRL of [ in a memory card ] is considered as the configuration which updates data serially at the time of distribution. Moreover, management of the inhibited class list CRL of [ in a memory card ] is considered as the configuration which can alter the inhibited class list data CRL from an upper level neither with a file system nor an application program by recording on a tamper REJISUTANTO module (Tamper Resistance Module) within a memory card independently of an upper level etc. Consequently, the protection of copyrights about data can be made firmer.  
<BR>[0088]

The open cryptographic keys KPpn and KPMci of a proper are formed in a portable telephone and a memory card, respectively, and the open cryptographic keys KPpn and KPMci can be decoded to a portable telephone, respectively with the secrecy decode key Kpn of a proper, and the secrecy decode key Kmci of a memory card proper. These disclosure cryptographic key and a secrecy decode key have a different value for every class of every class of portable telephone, and memory card. These open cryptographic keys and a secrecy decode key are named generically, and a class key is called.  
<BR>[0089]

Moreover, Crtfn and Cmc1 are prepared, respectively as a data playback terminal (portable telephone) and a class certificate of a memory card. These class certificates have different information for every class of a memory card and a contents playback terminal. To the class key with which the code with a class key was broken, namely, the secrecy decode key was acquired, it is listed by the inhibited class list and set as the prohibition object of license issuance.  
<BR>[0090]

The open cryptographic key and class certificate of these memory cards and a contents playback terminal proper are recorded [ the authentication data {KPMci//Cmc1} KPma and in the form of {KPpn//Crtfn} KPma ] on a memory card and a data playback terminal (portable telephone), respectively at the time of shipment. Although the back is explained to a detail, KPma is an open authentication key common to the whole distribution system.  
<BR>[0091]

```

<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web.cgi-ejje?u=http%3A%2F%2Fwww4.ipd
l.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B
%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D0000006"
TARGET="tjitemdrw">Drawing 4</A>
is drawing which summarizes the property of the key in connection with encryption,
and is explained in the data distribution system shown in
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web.cgi-ejje?u=http%3A%2F%2Fwww4.ipd
l.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B
%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D0000003"
TARGET="tjitemdrw">drawing 1</A>
.
<BR>[0092]

```

As a cryptographic key for the nondisclosure in the data transfer between the outside of a memory card, and a memory card, whenever distribution of contents data and playback are performed, the common keys Ks1-Ks3 generated in the distribution server 30, a portable telephone 100, and a memory card 110 are used.

```

<BR>[0093]

```

here, the common keys Ks1-Ks3 are the unit of the communication link between a distribution server, a portable telephone, or a memory card, or the unit of access -- "quote;-- it is the common key of a proper generated in every session"quote;, and suppose that these common keys Ks1-Ks3 are also called a "quote;session key"quote;; to below.

```

<BR>[0094]

```

These session keys Ks1-Ks3 are managed by a distribution server, a portable telephone, and the memory card by having the value of a proper for every communication link session. Specifically, the session key Ks1 is generated for every distribution session by the distribution server. The session key Ks2 is generated for every distribution session and playback session by the memory card, and the session key Ks3 is generated for every playback session in a portable telephone. In each session, the security reinforcement in a session can be raised by delivering and receiving these session keys, and transmitting a license key etc. in response to the session key generated by other devices, after performing encryption by this session key.

```

<BR>[0095]

```

Moreover, the secrecy decode key Km of a proper exists for every memory card which can decode the data enciphered as a key for managing data processing in a memory card 110 by open cryptographic key Kpm which is called a memory card, and which is set up for every medium, and the open cryptographic key Kpm.

```

<BR>[0096]

```

```

<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web.cgi-ejje?u=http%3A%2F%2Fwww4.ipd
l.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B
%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D0000007"
TARGET="tjitemdrw">Drawing 5</A>
is the outline block diagram showing the configuration of a license server 10 shown
in
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web.cgi-ejje?u=http%3A%2F%2Fwww4.ipd
l.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B
%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D0000003"
TARGET="tjitemdrw">drawing 1</A>
.
<BR>[0097]

```



The information database 304 for a license server 10 to hold the data which enciphered contents data according to the predetermined method, and delivery information, such as License ID,  
 The accounting database 302 for holding the accounting information which followed the access initiation to contents data for every cellular-phone user,  
 The CRL database 306 which manages the inhibited class list CRL, and the menu database 307 holding the menu of the contents data held at the information database,  
 The distribution record database 308 holding the transaction ID which specifies distribution of contents data, a license key, etc.,  
 A bus BS 1 is minded for the data from the information database 304, the accounting database 302, the CRL database 306, the menu database 307, and the distribution record database 308. A receipt,  
 It has the data-processing section 310 for performing predetermined processing, and the communication device 350 for performing data transfer between the distribution carrier 20 and the data-processing section 310 through a communication network.  
 <BR>[0098]

The distribution control section 315 for the data-processing section 310 to control actuation of the data-processing section 310 according to the data on a bus BS 1,  
 The session key generating section 316 for being controlled by the distribution control section 315 and generating the session key Ks1 at the time of a distribution session,  
 The authentication key attaching part 313 holding the open authentication key for decoding the authentication data KPma for the authentication sent from the memory card and the portable telephone {KPMci//Cmci},  
 The authentication data KPma for the authentication sent from the memory card and the portable telephone {KPMci//Cmci} are received through a communication device 350 and a bus BS 1.  
 The decode processing section 312 which performs decode processing with the open authentication key KPma from the authentication key attaching part 313,  
 The session key Ks1 generated from the session key generating section 316 is enciphered using the open cryptographic key KPMci obtained by the decode processing section 312.  
 The encryption processing section 318 for outputting to a bus BS 1 and the decode processing section 320 which performs decode processing in response to the data transmitted after being enciphered by the session key Ks1 from a bus BS 1 are included.  
 <BR>[0099]

The data-processing section 310 contains the encryption processing section 326 for enciphering further the license key Kc and the playback length AC 2 which are given from the distribution control section 315 by the open cryptographic key KPM of the memory card proper obtained by the decode processing section 320, and the encryption processing section 328 for enciphering further and outputting the output of the encryption processing section 326 to a bus BS 1 by the session key Ks2 to which it is given from the decode processing section 320.  
 <BR>[0100]

About the actuation in the distribution session of a license server 10, the back is explained to a detail using a flow chart.  
 <BR>[0101]

<A  
 HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran\_web.cgi\_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D0000008"  
 TARGET="tjitemdrw">Drawing 6</A>  
 is an outline block diagram for explaining the configuration of the portable telephone 100 shown in

<A  
 HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran\_web.cgi\_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D0000003"  
 Page 17

TARGET="tjitemdrw">drawing 1</A>

<BR>[0102]

A portable telephone 100 contains the controller 1106 for controlling actuation of a portable telephone 100 through the bus BS 2 and Bus BS 2 for performing data transfer of the transceiver section 1104 for changing into baseband signaling in response to the signal from the antenna 1102 for receiving the signal by which a radio transmission is carried out with a cellular-phone network, and an antenna 1102, or modulating the data from a portable telephone, and giving an antenna 1102, and each part of a portable telephone 100.

<BR>[0103]

A portable telephone 100 contains the voice playback section 1112 for reproducing voice further based on the received data given through a database BS 2 in the display 1110 and the usual call actuation for giving a cellular-phone user the information outputted from the key stroke section 1108 and the controller 1106 grade for giving the directions from the outside to a portable telephone 100 as vision information.

<BR>[0104]

A portable telephone 100 contains the terminal 1114 for outputting further the output of DA converter 1113 which changes the output of the voice playback section 1112 into an analog signal from a digital signal, and DA converter 1113 to an external output unit etc.

<BR>[0105]

A portable telephone 100 contains the microphone 1115 which inputs the sound signal about which the user of a portable telephone 100 spoke, A-D converter 1116 which changes the sound signal from a microphone 1115 into a digital signal from an analog signal, and the voice coding section 1117 which encodes according to a predetermined method and gives the digital signal from A-D converter 1116 to a bus BS 2 in the further usual call actuation.

<BR>[0106]

A portable telephone 100 includes the memory interface 1200 for controlling transfer of the data between the removable memory cards 110, the memory cards 110, and Buses BS 2 for memorizing the contents data (music data) from the distribution server 30, and carrying out decryption processing further.

<BR>[0107]

a portable telephone -- 100 -- further -- a portable telephone -- a class (class) -- every -- respectively -- setting up -- having -- disclosure -- a cryptographic key -- Kpp -- one -- and -- a class -- a certificate -- Crtf -- one -- disclosure -- decode -- a key -- Kpma -- decoding -- things -- the -- justification -- it can attest -- a condition -- having enciphered -- authentication -- data -- {- Kpp -- one -- /- /- Crtf -- one -} -- Kpma -- holding -- authentication -- data-hold -- the section -- 1202 -- containing .

Here, the class n of a portable telephone (Data Terminal Equipment) 100 presupposes that it is n = 1.

<BR>[0108]

A portable telephone 100 contains Kp1 attaching part 1204 which holds further Kp1 which is the decode key of a portable telephone (contents regenerative circuit) proper, and the decode processing section 1206 which obtains the session key Ks2 which decoded carrier beam data by Kp1 from the bus BS 2, and was generated by the memory card 110.

<BR>[0109]

A portable telephone 100 further

The session key generating section 1210 which generates the session key Ks3 for enciphering the data which set and are carried out on a bus BS 2 between memory cards 110 in the playback session which reproduces the contents data memorized by

the memory card 110 with a random number etc.,  
 The encryption processing section 1208 which enciphers the generated session key Ks3 by the session key Ks2 obtained by the decode processing section 1206, and is outputted to a bus BS 2 is included.  
 <BR>[0110]

A portable telephone 100 contains further the decode processing section 1212 which decodes and outputs the data on a bus BS 2 by the session key Ks3.  
 <BR>[0111]

The decode processing section 1214 which decodes a portable telephone 100 further with the license key Kc acquired from the bus BS 2 from the decode processing section 1212 in response to encryption contents {data Data} Kc, and outputs contents data,  
 The music playback section 1216 for reproducing contents data in response to the output of the decode processing section 1214,  
 DA converter 1218 which changes the output of the music playback section 1216 into an analog signal from a digital signal,  
 The switch 1222 for outputting from a terminal 1114 or a terminal 1220 selectively in response to the output of DA converter 1113 and DA converter 1218 according to a mode of operation,  
 In response to the output of a switch 1222, the connection terminal 1224 for connecting with a head telephone 130 is included.  
 <BR>[0112]

In addition, in

<A  
 HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran\_web.cgi\_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000008"  
 TARGET="tjitemdrw">drawing 6</A>  
 , for the simplification of explanation, only the block in connection with distribution and playback of this invention of music data is indicated among portable telephones, and the publication is omitted in part about the block about the call function with which the portable telephone is originally equipped.  
 <BR>[0113]

About the actuation in each session of each component of a portable telephone 100, the back is explained to a detail using a flow chart.  
 <BR>[0114]

<A  
 HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran\_web.cgi\_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000009"  
 TARGET="tjitemdrw">Drawing 7</A>  
 is an outline block diagram for explaining the configuration of a memory card 110. Although Kpmc1 and kmci are prepared in a memory card and the class certificate Cmc1 of a memory card is formed in it as the open cryptographic key and secrecy decode key of a proper as already explained, in a memory card 110, these shall be expressed with the natural number i= 1, respectively.  
 <BR>[0115]

Therefore, the authentication data-hold section 1400 in which a memory card 110 holds the authentication data {Kpmc1/Cmc1} Kpma,  
 Kmc1 attaching part 1402 holding Kmci which is the decode key of the proper set up for every class of memory card,  
 Kml attaching part 1421 holding the secrecy decode key Kml set as a proper for every memory card and Kpm1 attaching part 1416 holding the open cryptographic key Kpm1 which can be decoded by Kml are included.  
 authentication -- data-hold -- the section -- 1400 -- a memory card -- a class -- and -- a class -- every -- respectively -- setting up -- having -- secrecy -- a cryptographic key -- Kpmc -- one -- and -- a class -- a certificate -- Cmc -- one --

disclosure -- authentication -- a key -- KPma -- decoding -- things -- the --  
 justification -- it can attest -- a condition -- having enciphered -- authentication  
 -- data -- {-- KPmc -- one -- /-- /-- Cmc -- one --} -- KPma -- \*\*\*\*\* -- holding .  
 <BR>[0116]

Thus, by preparing the cryptographic key of a recording device called a memory card,  
 it becomes possible to perform management of the distributed contents data or the  
 enciphered license key per memory card so that it may become clear by the following  
 explanation.  
 <BR>[0117]

The interface 1423 with which a memory card 110 delivers further and receives a  
 signal through a terminal 1201 between the memory interfaces 1200,  
 The bus BS 3 which exchanges a signal between interfaces 1423  
 The secrecy decode key Kmcl of a proper is received from Kmcl attaching part 1402  
 for every class of the data given to a bus BS 3 from an interface 1423 to memory  
 card.  
 The decode processing section 1404 which outputs the session key Ks1 which the  
 distribution server 30 generated in the distribution session to Contact Pa,  
 The decode processing section 1408 which performs decode processing by KPma from the  
 data given to a bus BS 3 in response to the authentication key KPma from the KPma  
 attaching part 1414, and outputs a decode result to the encryption processing  
 section 1410,  
 The encryption processing section 1406 which enciphers the data selectively given by  
 the change-over switch 1444, and is outputted to a bus BS 3 with the key selectively  
 given by the change-over switch 1442 is included.  
 <BR>[0118]

The session key generating section 1418 in which a memory card 110 generates the  
 session key Ks2 in each session of distribution and playback further,  
 The encryption processing section 1410 which enciphers the session key Ks2 which the  
 session key generating section 1418 outputted by the open cryptographic keys Kppn  
 and KPmc obtained by the decode processing section 1408, and is sent out to a bus  
 BS 3,  
 It decodes by the session key Ks2 obtained from the session key generating section  
 1418 in response to the data enciphered by the session key Ks2 from the bus BS 3,  
 and the decode processing section 1412 which sends out a decode result to a bus BS 4  
 is included.  
 <BR>[0119]

The decode processing section 1422 for a memory card 110 to decode the data on a bus  
 BS 3 further with the open cryptographic key KPm1 and the secrecy decode key Km1 of  
 memory card 110 proper which makes a pair,  
 while storing in response to the inhibited class list data CRL updated serially from  
 a bus BS 4 by data CRL\_dat for the renewal of a version of an inhibited class list  
 Encryption contents data {data} The memory 1415 for storing in response to Kc and  
 additional information Data-inf from a bus BS 3 is included.  
 Memory 1415 is constituted by semiconductor memory.  
 Moreover, memory 1515 consists of data area 1415B which recorded CRL field 1415A  
 which recorded the inhibited class list CRL, Header containing content ID,  
 encryption contents {data Data} Kc, and related information Data-inf of encryption  
 contents data.  
 <BR>[0120]

A memory card 110 contains the license information attaching part 1440 for holding  
 further the license acquired by the decode processing section 1422, and the  
 controller 1420 for performing data transfer between the exteriors through a bus BS  
 3, and controlling actuation of a memory card 110 in response to playback  
 information etc. between buses BS 4.  
 <BR>[0121]

The license information attaching part 1440 has a bank of N individual (N: natural  
 number), and holds the license corresponding to each license for every bank.  
 Page 20

<BR>[0122]

In addition, in

<A

HREF="http://www4.ipdi.ncipi.go.jp/cgi-bin/tran\_web CGI-ejje?u=http%3A%2F%2FWww4.ipd  
l.ncipi.go.jp%2FTokujitu%2Ftjitmedmrw.ipdl%3FN00000%3D237%26N00000%3D1E%5FN%2F%3B%3E%3  
%36%3E7%3D8%2F%2E%2F%26N0001%3D1%26N005%26%3DN9%26N0553%3D000009"

TARGET="tjitemdrw">drawing 7</A>

the field enclosed with a continuous line shall be included in the module TRM for making impossible read-out of the data in the circuit which exists in the field to a third party etc. by elimination of an in-house data, or destruction of an internal circuitry, if unjust opening processing from the outside etc. is performed in a memory card 110.

Generally such a module is a tamper resistance module (Tamper Resistance Module).

<BR>[0123]

Of course, it is good also as a configuration incorporated in Module TRM also including memory 1415.

However, since each playback information required for the playback currently held in memory 1415 by considering as a configuration as shown in

 $\leq A$ 

HREF="http://www4.ipdi.ncipi.go.jp/cgi-bin/tran\_web CGI\_ejje?u=http%3A%2F%2Fwww4.ipd  
l.ncipi.go.jp%2F%2FTokujitu%2FTjitemredw.ipdl%3FN00000%3D23%726N00500%3DE1E5FN%3E2F%3B%3E3B  
%3F6%3E7%3D8%2F%2F%2FE2%2F6N0001%3D12%26N0552%3DD9%26N0553%3D000009"

TARGET="tjitemdraw">drawing 7</A>

is data encrypted, since a third party does not need to form memory 1415 in an expensive tamper resistance module impossible as for playing music, he has the advantage that a manufacturing cost is reduced, only by the data in this memory 1415.

<BR>[0124]

Henceforth, for simplification, the access-control information AC 1 shall restrict only the playback length which is the control information which specifies the length when the regenerative-circuit control information AC 2 is refreshable only for the count of playback which is the control information which restricts the count of playback, and shall call the access-control information AC 1 and the regenerative-circuit control information AC 2 the count limit AC 1 of playback, and the playback length AC 2, respectively.

&lt;BR&gt;[0125]

with reference to

<A

HREF="http://www4.ipd1.ncipi.go.jp/cgi-bin/tran\_web CGI\_ejje?u=http%3A%2F%2Fwww4.ipd1.ncipi.go.jp%2Ftokujitu%2Fjittemdaru.ipd1%3FNO0000%3D23%26NO5000%3DL1E5FN%2F%3B%3E%3B%3F%3E7%3D8%2F%2F%2F%2F%26NO0001%3D12%26NO5523%3D9%26NO5533%3D0000010

TARGET="tjitemdrw">drawing 8</A>

various kinds of conditions in the memory card 110 on which encryption contents  
[data data] Kc and the license which consists of the license key Kc, the count limit  
AC 1 of playback, and playback length AC2 grade were recorded are explained.

In addition, in

 $\leq A$ 

HREF="http://www4.ipd1.ncipi.go.jp/cgi-bin/tran\_web CGI\_ejje?u=http%3A%2F%2Fwww4.ipd1.ncipi.go.jp%2Ftokujitu%2Ftjitemdwr.ipd1%3F0N0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F%3E%3DB%2F%2F%2F%2F%26N0001%3D1%26N0552%3D99%26N0553%3D0000010

TARGET="tjitemdrw">drawing 8</A>

the case where there is no limit in the count limit AC 1 of playback is expressed with "FF", and the case where there is no limit in the playback length AC 2 is expressed with "00".

Encryption contents {data Data} KC and a license are recorded on the memory card 110. and (a) of

 $\leq A$ 

CA  
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran\_web CGI\_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FNO000%3D237%26NO500%3D1E%5FN%2F%3B%3E%3B

%3F6%3E7%3D8%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000010"

TARGET="tjitemdrw">drawing 8</A>

shows the case where encryption contents {data Data} Kc and a license are newly received from the distribution server 30.

Moreover, encryption contents {data Data} Kc and the license key Kc exist, and (b) of

<A

HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran\_web.cgi\_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000010"

TARGET="tjitemdrw">drawing 8</A>

shows the case where playback of encryption contents {data Data} Kc is restricted by the part and the count limit AC 1 of playback.

Furthermore, encryption contents {data Data} Kc and a license are recorded, and (c) of

<A

HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran\_web.cgi\_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000010"

TARGET="tjitemdrw">drawing 8</A>

shows the case where the license which reproduces a part of encryption contents {data Data} Kc(s) is not recorded.

<BR>[0126]

Encryption contents data:{Data(55019930112)} Kc specified by content ID:55019930112, and 55019951013 and 55019630122 with reference to (a) of

<A

HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran\_web.cgi\_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000010"

TARGET="tjitemdrw">drawing 8</A>

{55019930112},

{Data (55019951013)} Kc (55019951013),

{Data (55019630122)} Kc (55019630122),

The license key for decoding the encryption contents data: AAF53951046FD356ABCC,

96F539510456AB332C55, and F6F53695104AF3323C31 are recorded.

Moreover, content ID: Although the encryption contents data specified by 55019951013 and 55019630122 have the count limit AC 1 of playback, and the unrestricted playback

length AC 2, the playback length AC 2 of the count limit AC 1 of playback of the encryption contents data specified by content ID:55019930112 is unrestricted 20

times.

Therefore, the license over three encryption contents {data Data} Kc(s) recorded on data area 1415B is recorded on the license information attaching part 1440.

<BR>[0127]

(b) of

<A

HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran\_web.cgi\_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000010"

TARGET="tjitemdrw">drawing 8</A>

-- referring to -- content ID: -- license key:AAF53951046FD356ABCC for decoding encryption contents data:{Data(55019930112)} Kc (55019930112) specified by

55019930112 and 55019951013, {Data(55019951013)} Kc (55019951013), and its

encryption contents data and 96F539510456AB332C55 are recorded.

Moreover, content ID: Although the encryption contents data specified by 55019951013 have the count limit AC 1 of playback, and the unrestricted playback length AC 2,

the playback length AC 2 of the count limit AC 1 of playback of the encryption contents data specified by content ID:55019930112 is unrestricted 0 times.

Therefore, as for one encryption contents data, the license is not recorded on the license information attaching part 1440 between two encryption contents {data Data}

Kc(s) recorded on data area 1415B.

<BR>[0128]

(c) of

<A  
 HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran\_web.cgi\_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D0000010"  
 TARGET="tjitemdrw">drawing 8</A>  
 -- referring to -- content ID: -- license key:AAF53951046FD356ABCC for decoding encryption contents data:{Data(55019930112)} Kc (55019930112) specified by 55019930112 and 55019951013, {Data(55019951013)} Kc (55019951013), and its encryption contents data and 96F539510456AB332C55 are recorded.  
 Moreover, content ID: The encryption contents data specified by 55019951013 have the count limit AC 1 of playback, and the unrestricted playback length AC 2, and the playback length AC 2 of the count limit AC 1 of playback of the encryption contents data specified by content ID:55019930112 is unrestricted 20 times.  
 Furthermore, content ID: Although encryption contents data:{Data(55019630122)} Kc (55019630122) specified by 55019630122 is recorded on data area 1415B, the license which consists of the license key Kc for reproducing the encryption contents data, the count limit AC 1 of playback, and the playback length AC 2 is not recorded on the license information attaching part 1440.  
 Therefore, the license over one encryption contents data does not exist among three encryption contents {data Data} Kc(S) recorded on data area 1415B.  
 <BR>[0129]

As explained with reference to

<A  
 HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran\_web.cgi\_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D0000010"  
 TARGET="tjitemdrw">drawing 8</A>  
 , various kinds of conditions exist in a memory card 110 by whether the encryption contents data {Data} Kc, the license key Kc, the count limit AC 1 of playback, and the playback length AC 2 are recorded.  
 <BR>[0130]

Next, a portable telephone 100 is equipped with the memory card 110 on which encryption contents {data Data} Kc, the license key Kc, etc. were recorded in various kinds of condition, and actuation when request to receipt of encryption contents data is carried out from the user of a portable telephone 100 is explained.  
 <BR>[0131]

<A  
 HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran\_web.cgi\_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D0000010"  
 TARGET="tjitemdrw">Drawing 9</A>  
 -  
 <A  
 HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran\_web.cgi\_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D0000010"  
 TARGET="tjitemdrw">drawing 12</A>  
 are the 1st for explaining the distribution actuation (henceforth a distribution session) generated at the time of the purchase of the encryption contents data in the data distribution system shown in  
 <A  
 HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran\_web.cgi\_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D0000003"  
 TARGET="tjitemdrw">drawing 1</A>  
 - the 4th flow chart.  
 <BR>[0132]

If the distribution demand of contents data is made through the key stroke section 1108 with reference to

```
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web.cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000011"
TARGET="tjitemdrw">drawing 9</A>
from the user of a portable telephone 100, a portable telephone 100 will transmit the Request to Send of a contents menu to the distribution server 30 (step S70).
If the Request to Send of a contents menu is received through a communication device 350 and a bus BS 1 (step S72), from the menu database 307, read-out will be minded for a contents menu, and the distribution control section 315 of the distribution server 30 will mind a bus BS 1 and a communication device 350 for the read contents menu through a bus BS 1, and will transmit to a portable telephone 100 (step S74).
A portable telephone 110 receives a contents menu by the transceiver section 1104, and a controller 1106 displays a contents menu on a display 1110 (step S76).
<BR>[0133]
```

If it does so, the contents menu 60 shown in

```
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web.cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000015"
TARGET="tjitemdrw">drawing 13</A>
will be displayed on the display 1110 of a portable telephone 100.
A user chooses the numbers 001, 002, and 003 of the contents menu 60, and the encryption contents data which wish to distribute by choosing ...
The shift section 1111 for shifting to another screen is formed in the display 1110.
A user clicks the shift section 1111, when the encryption contents data wished to have into the contents menu 60 displayed on the display 1110 are not displayed.
The address for shifting to another screen is included in the shift section 1111.
<BR>[0134]
```

It is required that a controller 1106 will transmit the address included in the shift section 1111 to the distribution server 30 through the transceiver section 1104, and the controller 1106 of a portable telephone 100 will transmit another screen if it judges whether it is the no as which contents were chosen (step S78) and the shift section 1111 is clicked.

And steps S70-S78 are repeated.

That is, two or more screens which consist of the contents menu 60 are arranged hierarchical, the contents menu is constituted, and although each screen is the encryption contents data and the same genre from which a genre differs, it is constituted by the contents menu which consists of other encryption contents data etc.

```
<BR>[0135]
```

And when the encryption contents data to wish to have are not contained in the contents menu sent by two or more screens from the distribution server 30, distribution actuation shifts to step S170, and distribution actuation is ended.

```
<BR>[0136]
```

The contents menu 60 contains the content ID for specifying encryption contents data, and when encryption contents data are chosen in step S78, the content ID of the encryption contents data chosen from the contents menu is extracted (step S80).

```
<BR>[0137]
```

And the purchase conditions AC for purchasing the license of encryption contents data through the key stroke section 1108 are inputted (step S82).

That is, in order to purchase the license key KC which decodes selected encryption contents data, the count limit AC 1 of playback and the playback length AC 2 of encryption contents data are set up, and the purchase conditions AC are inputted.

```
<BR>[0138]
```



If the purchase conditions AC of encryption contents data are inputted, a controller 1106 will search whether encryption contents {data Data} Kc which has the same content ID as the content ID to selected encryption contents data is recorded on the memory card 110 (step S84).

In this case, a controller 1106 transmits the content ID corresponding to selected encryption contents data to a memory card 110 through the memory interface 1200. The controller 1420 of a memory card 110 searches whether the encryption contents data as which the user chose content ID from the contents menu by whether it is in agreement with the content ID by which a receipt and its received content ID are contained in Header1424 of memory 1415 are recorded on the memory card 110 from the portable telephone 100 through the interface 1423 and the bus BS 3.  
<BR>[0139]

In this case, if signature data using the Hash Function etc. considering Header and Data-inf which were recorded on the memory 1415 of a memory card 110, and {Data} Kc as one data stream are collectively dealt with as shown in

```
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web.cgi-ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FNO000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000010"
TARGET="tjitemdrw">drawing 14</A>
```

, reorganization of content ID can be prevented.  
what is necessary is just to perform the check of a signature also about the thing corresponding to the time of inspection of content ID.  
<BR>[0140]

And a controller 1106 stands flag "Yes"; for acquiring data from the distribution server 30, when it judges whether selected encryption contents data are recorded on the memory card 110 (step S86) and encryption contents data are not recorded on a memory card 110 (step S88).

The check of a license is performed when encryption contents data are recorded on the memory card 110 (step S90).

That is, the check of a license is performed by whether the license key Kc is recorded on the memory card 110 as having explained with reference to

```
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web.cgi-ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FNO000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000010"
TARGET="tjitemdrw">drawing 8</A>
```

, or playback of encryption contents data is not restricted by the count limit AC 1 of playback, and the playback length AC 2.

When a license does not exist, it shifts to step S94.

When a license exists and encryption contents data can be reproduced, a controller 1106 displays "license simple substance purchase"; on a display 1110, and it is sure of the intention of whether to purchase only a license alone (step S92).

If directions of the purport which does not purchase only a license are inputted from the key stroke section 1108, a controller 1106 will shift to step S170, and will end distribution actuation of encryption contents data.

A controller 1106 will stand flag "No"; which does not acquire data from the distribution server 30, if directions of the purport which purchases only a license alone are inputted from the key stroke section 1108 (step S94).

<BR>[0141]

Next, with reference to

```
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web.cgi-ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FNO000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000010"
TARGET="tjitemdrw">drawing 10</A>
```

, the distribution request by assignment of content ID (step S80 reference) that the user extracted the portable telephone 100 by choosing encryption contents data is made (step S100).

<BR>[0142]

In a memory card 110, the authentication data {KPMc1//Cmc1} KPma are outputted from the authentication data-hold section 1400 according to this distribution request (step S102).  
<BR>[0143]

In addition to the authentication data KPma for the authentication from a memory card 110 {KPMc1//Cmc1}, a portable telephone 100 transmits the data AC of content ID and license purchase conditions to the distribution server 30 (step S104).  
<BR>[0144]

In the distribution server 30, content ID, the authentication data {KPMc1//Cmc1} KPma, and the data AC of license purchase conditions are received from a portable telephone 100 (step S106), and decode processing is performed for the authentication data outputted from the memory card 110 in the decode processing section 312 with the open authentication key KPma (step S108).  
<BR>[0145]

The distribution control section 315 performs authentication processing which judges whether the authentication data which gave the code for proving the justification in the engine of normal were received, in order to attest that whether processing having been performed normally and a memory card 110 hold the open cryptographic key KPMc1 and certificate Cmc1 from a memory card of normal from the decode processing result in the decode processing section 312 (step S110). When it is judged that it is just authentication data, the distribution control section 315 recognizes and receives the open cryptographic key KPMc1 and a certificate Cmc1.  
And it shifts to the next processing (step S112).  
In not being just authentication data, it supposes un-recognizing, and it ends processing without receiving the open cryptographic key KPMc1 and a certificate Cmc1 (step S170).  
<BR>[0146]

If it is recognized as a result of authentication that it is the device of normal, when, as for the distribution control section 315, these class certificates are set as the object of an inhibited class list by referring for whether next the class certificate Cmc1 of a memory card 110 is listed by the inhibited class list CRL to the CRL database 306, a distribution session is ended here (step S170).  
<BR>[0147]

On the other hand, when the class certificate of a memory card 110 is outside the object of an inhibited class list, it shifts to the next processing (step S112).  
<BR>[0148]

If it is checked that it is access from the portable telephone equipped with a memory card with just authentication data as a result of authentication, and a class is outside the object of an inhibited class list, in the distribution server 30, the distribution control section 315 will generate the transaction ID which is Control Code for specifying distribution (step S113).  
Moreover, the session key generating section 316 generates the session key Ks1 for distribution.  
The session key Ks1 is enciphered by the encryption processing section 318 by the open cryptographic key KPMc1 corresponding to the memory card 110 obtained by the decode processing section 312 (step S114).  
<BR>[0149]

Transaction ID and the enciphered session key Ks1 are outputted outside through a bus BS 1 and a communication device 350 as transaction ID//{Ks1} Kmcl (step S116).  
<BR>[0150]

When the decode processing section 1404 carries out decode processing of the received data with which it was given to the bus BS 3 through the memory interface 1200 in the memory card 110 when the portable telephone 100 received transaction

ID://{Ks1} Kmcl (step S118) with the secrecy decode key Kmcl of memory card 110 proper held at an attaching part 1402, the session key Ks1 is decoded and extracted (step S120).  
<BR>[0151]

A controller 1420 directs generation of the session key Ks2 generated in a memory card 110 at the time of distribution actuation to the session key generating section 1418, if acceptance of the session key Ks1 generated by the distribution server 30 is checked.  
<BR>[0152]

Moreover, in a distribution session, a controller 1420 extracts data CRL\_dat of the inhibited class list currently recorded on the memory 1415 in a memory card 110 from memory 1415, and outputs it to a bus BS 4.  
<BR>[0153]

By the session key Ks1 given from the decode processing section 1404 through the contact Pa of a change-over switch 1442, the encryption processing section 1406 enciphers data CRL\_dat of the session key Ks2 given by switching the contact of change-over switches 1444 and 1446 one by one, the open cryptographic key Kpm1, and an inhibited class list as one data stream, and outputs {Ks2//Kpm1//CRL\_dat} Ks1 to a bus BS 3 (step S122).  
<BR>[0154]

Encryption data {Ks2//Kpm1//CRL\_ver} Ks1 outputted to the bus BS 3 is outputted to a portable telephone 100 through an interface 1423, a terminal 1201, and the memory interface 1200 from a bus BS 3, and is transmitted to the distribution server 30 from a portable telephone 100 (step S124).  
<BR>[0155]

The distribution server 30 receives transaction ID://{Ks2//Kpm1//CRL\_dat} Ks1, performs decode processing by the session key Ks1 in the decode processing section 320, and receives data CRL\_dat of the inhibited class list in the open cryptographic key Kpm1 and memory card 110 of the session key Ks2 and memory card 110 proper which were generated by the memory card 110 (step S126).  
<BR>[0156]

The distribution control section 315 generates License ID, the access-restriction information AC 1, and the playback length AC 2 according to the data AC of the content ID acquired at step S106, and license purchase conditions (step S128). Furthermore, the license key Kc for decoding encryption contents data is acquired from the information database 304 (step S130).  
<BR>[0157]

The distribution control section 315 gives the generated license Kc, i.e., a license key, the playback length AC 2, License ID, content ID, and the access-restriction information AC 1 to the encryption processing section 326.  
The encryption processing section 326 shifts to step S134, when it is judged for data CRL\_dat of the inhibited class list transmitted from the memory card 110 by the open cryptographic key Kpm1 of memory card 110 proper obtained by the decode processing section 320 in the distribution server 30 whether it is the newest and data CRL\_dat is judged to be the newest with reference to

<A  
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran\_web.cgi\_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000013"  
TARGET="tjitemdrw">drawing 11</A>  
(step S132) which enciphers a license.  
Moreover, when data CRL\_dat is not the newest, it shifts to step S137 (step S133).  
<BR>[0158]

When data CRL\_dat is judged to be the newest, the encryption processing section 328 Encryption data {Kc//AC2// license ID// content ID// AC1} outputted from the

encryption processing section 326 Km1 is enciphered by the session key Ks2 generated in the memory card 110.

Encryption data {Kc//AC2// license ID// content ID// {AC1} Km1} Ks2 is outputted to a bus BS 1.

And the distribution control section 315 transmits Kc//AC2// license ID// content ID// encryption data {{AC1} Km1} Ks2 on a bus BS 1 to a portable telephone 100 through a communication device 350 (step S134).

<BR>[0159]

And a portable telephone 100 receives Kc//AC2// license ID// content ID// encryption data {{AC1} Km1} Ks2 (step S135), and transmits it to a memory card 110 through a bus BS 2 and the memory interface 1200.

The decode processing section 1412 of a memory card 110 decodes Kc//AC2// license ID// content ID// encryption data {{AC1} Km1} Ks2 by the session key Ks2 generated by the receipt and the session key generating section 1418 through the terminal 1201 and the interface 1423, and receives Kc//AC2// license ID// content ID// {AC1} Km1 (step S136).

Then, it shifts to step S146.

<BR>[0160]

On the other hand, if it is judged in the distribution server 30 that CRL\_dat is not the newest, the distribution control section 315 will acquire data CRL\_dat of the newest inhibited class list from the CRL database 306 through a bus BS 1 (step S137).

<BR>[0161]

The encryption processing section 328 is enciphered by the session key Ks2 generated in the memory card 110 in response to the output of the encryption processing section 326, and newest data CRL\_dat of the inhibited class list which the distribution control section 315 supplies through a bus BS 1.

The encryption data outputted from the encryption processing section 328 are transmitted to a portable telephone 100 through a bus BS 1 and a communication device 350 (step S138).

<BR>[0162]

Thus, by exchanging the cryptographic key generated by the distribution server and the memory card, respectively, performing encryption using the cryptographic key which each received, and transmitting the encryption data to the other party, mutual recognition on data can be performed also in transmission and reception of each encryption data, and the security of a data distribution system can be raised.

<BR>[0163]

A portable telephone 100 receives transmitted encryption data {Kc//AC2// license ID// content ID// {AC1} Km1//CRL\_dat} Ks2 (step S140), and outputs it to a memory card 110 through the memory interface 1200.

In a memory card 110, the received data given to the bus BS 3 are decoded by the decode processing section 1412 through a terminal 1201 and an interface 1423.

The decode processing section 1412 decodes the received data of a bus BS 3 using the session key Ks2 given from the session key generating section 1418, and outputs them to a bus BS 4 (step S142).

<BR>[0164]

In this phase, encryption {license AC 1} Kc//AC2// license ID// content ID// Km1 which can be decoded with the secrecy decode key Km1 held at Km1 attaching part 1421, and CRL\_dat are outputted to a bus BS 4 (step S142).

The inhibited class list CRL of [ in memory 1415 ] is rewritten by the newest inhibited class list CRL\_dat received with directions of a controller 1420 (step S144).

<BR>[0165]

Steps S134, S135, and S136 are distribution actuation to the memory cards 110, such as the license key Kc in case inhibited class list CRL\_dat sent from the memory card 110 is the newest, and steps S137, S138, S140, S142, and S144 are distribution

actuation to the memory cards 110, such as the license key Kc in case inhibited class list CRL\_dat sent from the memory card 110 is not the newest. Thus, when checking in detail and not updating whether inhibited class list CRL\_dat sent from the memory card 110 is updated, By acquiring the newest inhibited class list CRL\_dat from the CRL database 306, and distributing to a memory card 110 The playback of encryption contents {data Data} Kc by the portable telephone with which the distribution of encryption contents {data Data} Kc to the memory card by which the license was broken was prevented, and the license was broken can be prevented.  
<BR>[0166]

After step S136 or step S144, encryption {license AC 1} Kc//AC2// license ID// content ID// Kml are decoded by directions of a controller 1420 with the secrecy decode key Kml in the decode processing section 1422, and a license (the license key Kc, License ID, content ID, the count limit AC 1 of playback, and playback length AC 2) is received by them (step S148).  
<BR>[0167]

A controller 1420 records a license on the license information attaching part 1440 (step S150).  
<BR>[0168]

with reference to

<A  
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran\_web.cgi\_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000014" TARGET="tjitemdrw">drawing 12</A>  
, the controller 1106 of a portable telephone 100 judges whether encryption contents data are acquired from the distribution server 30 with reference to the flag set in step S88 and step S94. And when not acquiring encryption contents data from the distribution server 30, it shifts to step S164, and when acquiring encryption contents data from the distribution server 30, it shifts to step S154.  
<BR>[0169]

when acquiring encryption contents data from the distribution server 30, a portable telephone 100 transmits the distribution demand of the Transaction ID and encryption contents data which were sent from the distribution server 30 to the distribution server 30 (step S154).  
<BR>[0170]

The distribution server 30 receives the distribution demand of Transaction ID and encryption contents data (step S156), from the information database 304, acquires encryption contents {data Data} Kc and additional information Data-inf, and outputs these data through a bus BS 1 and a communication device 350 (step S158).  
<BR>[0171]

A portable telephone 100 receives {Data} Kc//Data-inf, and receives encryption contents {data Data} Kc and additional information Data-inf (step S160). Encryption contents data {Data} Kc and additional information Data-inf are transmitted to the bus BS 3 of a memory card 110 through the memory interface 1200, a terminal 1201, and an interface 1423. In a memory card 110, encryption contents {data Data} Kc and additional information Data-inf which received are recorded on memory 1415 as it is (step S162).  
<BR>[0172]

It includes, also when it is judged that encryption contents data are not received from the distribution server 30 in step S152. And to the distribution server 30, from a memory card 110 Advice of transaction ID// distribution acceptance is transmitted (step S164). If transaction ID// distribution acceptance is received by the distribution server

30 (step S166)

Storing of the account data to the accounting database 302 and record in the distribution record database 308 of Transaction ID are performed, processing of distribution termination is performed (step S168), and the whole processing is completed (step S170).

<BR>[0173]

Thus, the memory card 110 with which the portable telephone 100 was equipped is the device of normal,

After checking that the open cryptographic keys Kp1 and Km1 which have enciphered and transmitted with the class certificate Cm1 are effective simultaneously

Each class certificate Cm1 can distribute contents data only to the distribution demand from the memory card which is not indicated by the inhibited class list, i.e., the class certificate list with which encryption by the open cryptographic keys Kp1 and Km1 was broken.

The distribution using the class key to an inaccurate memory card distributed and decoded can be forbidden.

<BR>[0174]

Moreover, according to the record situation of the encryption contents {data Data} encryption contents data {Data} Kc in a memory card 110 to the distribution server 30, the license key Kc, and count limit Acof playback 1 grade, only required distribution can be required of the distribution demand of Kc at the distribution server 30.

Consequently, useless distribution can be prevented.

<BR>[0175]

Next, the playback actuation in the portable telephone 100 of the contents data distributed to the memory card 110 with reference to

<A

HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran\_web.cgi\_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000017"  
TARGET="tjitemdrw">drawing 15</A>

and

<A

HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran\_web.cgi\_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000017"  
TARGET="tjitemdrw">drawing 16</A>

is explained.

with reference to

<A

HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran\_web.cgi\_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000017"  
TARGET="tjitemdrw">drawing 15</A>

, playback directions are inputted to a portable telephone 100 through the key stroke section 1108 with initiation of playback actuation from the user of a portable telephone 100 (step S200).

If it does so, a controller 1106 will input the authentication data {Kpp1//Crtf1} KPma into a memory card 110 for the authentication data {Kpp1//Crtf1} KPma through read-out and the memory interface 1200 through a bus BS 2 from the authentication data-hold section 1202 (step S201).

<BR>[0176]

If it does so, a memory card 110 will receive the authentication data {Kpp1//Crtf1} KPma (step S202).

And the decode processing section 1408 of a memory card 110 decodes the received authentication data {Kpp1//Crtf1} KPma with the open authentication key KPma held at the KPma attaching part 1414 (step S203), and a controller 1420 performs authentication processing from the decode processing result in the decode processing section 1408.

That is, authentication processing which judges whether the authentication data {Kppl/Crtf1} Kpma are authentication data of normal is performed (step S204). When it is not able to decode, a controller 1420 outputs authentication data a non-received output to the memory interface 1200 of a portable telephone 100 through data BS 3 and a terminal 1201 (step S206). When authentication data are able to be decoded, it judges whether a controller 1420 is contained in the inhibited class list data which the acquired certificate Crtf1 read from memory 1415 (step S205). In this case, ID is given to the certificate Crtf1 and a controller 1420 distinguishes whether ID of the received certificate Crtf1 exists in inhibited class list data. If a certificate Crtf1 is judged to be contained in inhibited class list data, a controller 1420 will output authentication data a non-received output to the memory interface 1200 of a portable telephone 100 through data BS 3 and a terminal 1201 (step S206).  
<BR>[0177]

When authentication data are not able to decode with the open authentication key Kpma in step S204, and when the certificate Crtf1 received in step S205 is contained in inhibited class list data, authentication data a non-received output is made. And the controller 1106 of a portable telephone 100 will display authentication data non-received data on a display 1110, if authentication data a non-received output is undergone through the memory interface 1200 (step S207).  
<BR>[0178]

In step S205, if a certificate Crtf1 is judged not to be contained in inhibited class list data, with reference to

<A  
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran\_web.cgi\_eije?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000018"  
TARGET="tjitemdrw">drawing 16</A>  
, the session key generating section 1418 of a memory card 110 will generate the session key Ks2 for playback sessions (step S208). And the cipher-processing section 1410 outputs {Ks2} Kp1 which enciphered the session key Ks2 from the session key generating section 1418 by the open cryptographic key Kppl decoded in the decode processing section 1408 to a bus BS 3 (step S209). If it does so, a controller 1420 will output {Ks2} Kp1 to the memory interface 1200 through a terminal 1201, and the controller 1106 of a portable telephone 100 will acquire {Ks2} Kp1 through the memory interface 1200. And Kp1 attaching part 1204 outputs the secrecy decode key Kp1 to the decode processing section 1206.  
<BR>[0179]

With the secrecy decode key Kp1 which was outputted from Kp1 attaching part 1204 and which is the open cryptographic key Kppl and a pair, the decode processing section 1206 decodes {Ks2} Kp1, and outputs the session key Ks2 to the cipher-processing section 1208 (step S210). If it does so, the session key generating section 1210 will generate the session key Ks3 for playback sessions, and will output the session key Ks3 to the cipher-processing section 1208 (step S211). The cipher-processing section 1208 enciphers the session key Ks3 from the session key generating section 1210 by the session key Ks2 from the decode processing section 1206, and outputs {Ks3} Ks2, and a controller 1106 outputs {Ks3} Ks2 to a memory card 110 through a bus BS 2 and the memory interface 1200 (step S212).  
<BR>[0180]

The decode processing section 1412 of a memory card 110 inputs {Ks3} Ks2 through a terminal 1201, an interface 1423, and a bus BS 3, decodes {Ks3} Ks2 by the session key Ks2 generated by the session key generating section 1418, and acquires the session key Ks3 generated in the portable telephone 100 (step S213).  
<BR>[0181]

According to acceptance of the session key Ks3, a controller 1420 checks the access-restriction information AC 1 to which it corresponds in the license information attaching part 1440 (step S214).  
<BR>[0182]

In step S214, by checking the access-restriction information AC 1 which is the information about the limit to access of memory, it ends playback actuation, in being in a condition [ that it is already unreproducible ], and it progresses to the following step, after updating the data of the access-restriction information AC 1 and updating the count of refreshable, when the count limit of playback has a limit (step S215).  
On the other hand, when the count limit of playback is not restricted by the access-restriction information AC 1, step S215 is skipped, and processing advances to the following step (step S216), without updating the count limit AC 1 of playback.  
<BR>[0183]

Moreover, when the content ID concerned of a request song does not exist in the license information attaching part 1440, it judges that it is in a condition [ being unreproducible ], and playback actuation is ended.  
<BR>[0184]

In step S214, when it is judged in the playback actuation concerned that it is reproducible, the license key Kc of a playback request song and the playback length AC 2 which were recorded on the license information attaching part 1440 are outputted on a bus BS 4 (step S216).  
<BR>[0185]

The license key Kc and the playback length AC 2 which were obtained are sent to the encryption processing section 1406 through the contact Pd of a change-over switch 1444.  
Through the contact Pd of a change-over switch 1442, by the carrier beam session key Ks3, the encryption processing section 1406 enciphers the carrier beam license key Kc and the playback length AC 2 from a bus BS 4, and outputs {Kc//AC2} Ks3 to a bus BS 3 from the decode processing section 1412 (step S217).  
<BR>[0186]

The encryption data outputted to the bus BS 3 are sent out to a portable telephone 100 through an interface 1423, a terminal 1202, and the memory interface 1200.  
<BR>[0187]

In a portable telephone 100, the decode processing section 1212 performs decode processing for encryption {Kc// data AC 2} Ks3 transmitted to a bus BS 2 through the memory interface 1200, and the license key Kc and the playback length AC 2 are received (step S218).  
The decode processing section 1212 transmits the license key Kc to the decode processing section 1214, and outputs the playback length AC 2 to a bus BS 2.  
<BR>[0188]

Through a bus BS 2, a controller 1106 receives the playback length AC 2, and checks reproductive propriety (step S219).  
<BR>[0189]

In step S219, when it is judged by the playback length AC 2 that playback is impossible, playback actuation is ended.  
<BR>[0190]

When it is judged in step S219 that it is refreshable, a controller 1106 requires encryption contents {data Data} Kc of a memory card 110 through the memory interface 1200.  
If it does so, the controller 1420 of a memory card 110 will acquire encryption contents {data Data} Kc from memory 1415, and will output it to the memory interface  
Page 32



1200 through a bus BS 3 and a terminal 1201 (step S220).

<BR>[0191]

The controller 1106 of a portable telephone 100 acquires encryption contents {data Data} Kc through the memory interface 1200, and gives encryption contents {data Data} Kc to the decode processing section 1214 through a bus BS 2.

And the decode processing section 1214 decodes encryption contents {data Data} Kc with the contents key Kc outputted from the decode processing section 1212, and acquires the contents data Data (step S221).

<BR>[0192]

And they are outputted to the music playback section 1216, and the decoded contents data Data reproduce contents data, and the music playback section 1216 changes a digital signal into an analog signal, and outputs DA converter 1218 to a terminal 1220.

And a switch 1222 chooses a terminal 1220, and through a terminal 1224, music data are outputted to a head telephone 130, and are reproduced (step S222).

Playback actuation is completed by this.

<BR>[0193]

with reference to

<A

HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran\_web.cgi\_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FNO0000%3D237%26NO500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000019"

TARGET="tjitemdrw">drawing 17</A>

, the example of distribution, such as encryption contents {data Data} Kc, the license key Kc, etc. according to record situations, such as encryption contents {data Data} Kc in a memory card 110 and the license key Kc, is explained.

with reference to (a) of

<A

HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran\_web.cgi\_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FNO0000%3D237%26NO500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000019"

TARGET="tjitemdrw">drawing 17</A>

, encryption contents data:{Data(55019930112)} Kc (55019930112), {Data(55019951013)} Kc (55019951013), {Data(55019630122)} Kc (55019630122), and each related information Data-inf are recorded on data area 14158 of a memory card 110.

Moreover, the license LS 1 of content ID:55019930112, transaction ID:000000000001, license key Kc:AAF53951046FD356ABCC, the count limit AC 1:00 of playback, and the playback length AC 2:00 and the license LS 2 of content ID:55019951013, transaction ID:000000003005, license key Kc:96F539510456AB332C55, count limit ACof playback1:FF, and the playback length AC 2:00 are recorded on license field 1415A.

And about the license LS 1, since the count limit AC 1 of playback is "00", encryption contents {data Data (55019930112)} Kc (55019930112) cannot be reproduced, namely, the condition that there is no license is shown. Moreover, about encryption contents {data Data (55019630122)} Kc (55019630122), content ID, the license key Kc, the count limit AC 1 of playback, and the playback length AC 2 are not recorded, but the condition that there is no license is shown. That is, the license LS 2 over encryption contents {data Data (55019951013)} Kc (55019951013) exists, and they are encryption contents {data Data (55019930112)} Kc (55019930112) and {data (55019630122)} it is in the situation that the license over Kc (55019630122) does not exist.).

<BR>[0194]

In the situation of a memory card 110 shown in (a) of

<A

HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran\_web.cgi\_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FNO0000%3D237%26NO500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000019"

TARGET="tjitemdrw">drawing 17</A>

, if the distribution demand of encryption contents {data Data} Kc specified by content ID:55019930112 from the user of a portable telephone 100 is inputted through

the key stroke section 1108, steps S70-S78 of

```
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web.cgi_ejje?u=http%3A%2F%2Fwww4.ipd
l.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B
%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000011"
TARGET="tjitemdrw">drawing 9</A>
will be performed, and content ID:55019930112 will be extracted (step S80).
And in step S82, the purchase conditions AC of the license made refreshable to
"20"; times are inputted.
And content ID: It is searched whether encryption contents {data Data} Kc specified
by 55019930112 is recorded on the memory card 110 (step S84).
<BR>[0195]
```

In this case, content ID: Since encryption contents {data Data} Kc specified by 55019930112 is recorded on the memory card 110 as encryption contents {data Data (55019930112)} Kc (55019930112), it shifts to step S90 through step S86 of

```
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web.cgi_ejje?u=http%3A%2F%2Fwww4.ipd
l.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B
%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000011"
TARGET="tjitemdrw">drawing 9</A>
```

And in step S90, it is judged according to a license whether encryption contents {data Data (55019930112)} Kc (55019930112) is refreshable. In this case, since the count limit AC 1 of playback is "00", encryption contents {data Data (55019930112)} Kc (55019930112) is unreproducible. Therefore, it shifts to step S94 from step S90. And after the flag of data acquisition "No" is set in step S94, only the license which makes "20"; times the count limit AC 1 of playback by step S100 - step S170 is distributed to a memory card 110 from the distribution server 30.

And as shown in (b) of

```
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web.cgi_ejje?u=http%3A%2F%2Fwww4.ipd
l.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B
%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000011"
TARGET="tjitemdrw">drawing 17</A>
, the count limit AC 1 of playback of license LS 1 is changed with "20";
Encryption contents {data Data (55019930112)} Kc (55019930112) is [ with this ]
reproducible with license LS 1.
<BR>[0196]
```

Moreover, in the situation of a memory card 110 shown in (a) of

```
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web.cgi_ejje?u=http%3A%2F%2Fwww4.ipd
l.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B
%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000011"
TARGET="tjitemdrw">drawing 17</A>
, if the distribution demand of encryption contents {data Data} Kc specified by
content ID:55012345678 from the user of a portable telephone 100 is inputted through
the key stroke section 1108, steps S70-S78 of
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web.cgi_ejje?u=http%3A%2F%2Fwww4.ipd
l.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B
%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000011"
TARGET="tjitemdrw">drawing 9</A>
will be performed, and content ID:55012345678 will be extracted (step S80).
then -- as the purchase conditions AC for a license -- AC1: -- those of FF and
AC2:00 without a playback limit are inputted (step S82).
And content ID: It is searched whether encryption contents {data Data} Kc specified
by 55012345678 is recorded on the memory card 110 (step S84).
In this case, content ID: Since encryption contents {data Data} Kc specified by
55012345678 is not recorded on a memory card 110, from step S86, it shifts to step
```

s88 and the flag of data acquisition = "Yes"; is set in step S88.  
<BR>[0197]

Then, step S100 - step S170 are performed, and content ID:55012345678, transaction ID:000005500345, license key Kc:C6F569510456AB333C4, count limit ACof playback1:FF, the playback length AC 2:00, encryption contents data:{data (55012345678)} Kc (55012345678), and related information DataD-inf (55012345678) are distributed and recorded on a memory card 110.

By this, a memory card 110 will be in the condition which shows in (c) of

<A  
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran\_web.cgi\_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FNO000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000019"

TARGET="tjitemdrw">drawing 17</A>  
, and will become reproducible [ encryption contents {data Data (55012345678)} Kc (55012345678) to which the user gave the distribution demand ].

<BR>[0198]

Furthermore, in the situation of a memory card 110 shown in (a) of

<A  
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran\_web.cgi\_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FNO000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000019"

TARGET="tjitemdrw">drawing 17</A>  
, if the distribution demand of encryption contents {data Data} Kc specified by content ID:55019630122 from the user of a portable telephone 100 is inputted through the key stroke section 1108, steps S70-S78 of

<A  
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran\_web.cgi\_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FNO000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000019"

TARGET="tjitemdrw">drawing 9</A>  
will be performed, and content ID:55019630122 will be extracted (step S80).

then -- as the purchase conditions AC for a license -- AC1: -- those of FF and AC2:00 without a playback limit are inputted (step S82).

And content ID: It is searched whether encryption contents {data Data} Kc specified by 55019630122 is recorded on the memory card 110 (step S84).

In this case, content ID: Since encryption contents {data Data} Kc specified by 55019630122 is recorded on the memory card 110, shift to step S90 from step S86.

And in step S90, it is judged according to a license whether encryption contents {data Data (55019630122)} Kc (55019630122) is refreshable.

In this case, since neither content ID nor the license key Kc nor the count limit AC 1 of playback nor the playback length AC is recorded on the memory card 110,

encryption contents {data Data (55019630122)} Kc (55019630122) is unreproducible. Therefore, it shifts to step S94 from step S90.

<BR>[0199]

And after the flag of data acquisition = "No"; is set in step S94, only the license made to have no playback limit by step S100 - step S170 is distributed to a memory card 110 from the distribution server 30.

And as shown in (d) of

<A  
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran\_web.cgi\_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FNO000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000019"

TARGET="tjitemdrw">drawing 17</A>

, content ID:55019630122, transaction ID:00000550339, license key Kc:F6F53695104AF3323C31, count limit ACof playback1:FF, and playback length:00 are recorded on license field 1415A of a memory card 110.

Encryption contents {data Data (55019630122)} Kc (55019630122) is reproducible with this.

<BR>[0200]

As mentioned above, according to record situations, such as encryption contents {data Data} Kc in a memory card 110, and the license key Kc, the user of a portable telephone 100 receives encryption contents {data Data} Kc, the license key Kc, etc. from the distribution server 30 to a memory card 110 using a portable telephone 100, can decode encryption contents {data Data} Kc with the license key Kc, and can be reincarnated.  
<BR>[0201]

When the user of a portable telephone 100 performs the distribution demand of encryption contents {data Data} Kc in the above, Although it was explained that encryption contents {data Data} Kc currently recorded on the memory card 110 was encryption contents data received from the distribution server 30 In this invention, not only this case but when only encryption contents {data Data} Kc is received from other than distribution server 30 and it records on a memory card 110, it is contained.  
<BR>[0202]

With reference to

```
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web.cgi_ejje?u=http%3A%2F%2Fwww4.ipd
l.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipd1%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B
%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000020"
TARGET="tjitemdrw">drawing 18</A>
and
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web.cgi_ejje?u=http%3A%2F%2Fwww4.ipd
l.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipd1%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B
%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000020"
TARGET="tjitemdrw">drawing 19</A>
, encryption contents {data Data} Kc is received from equipments other than
distribution server 30, and the case where the encryption contents {data Data} Kc is
recorded on a memory card 110 is explained.
<BR>[0203]
```

With reference to

```
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web.cgi_ejje?u=http%3A%2F%2Fwww4.ipd
l.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipd1%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B
%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000020"
TARGET="tjitemdrw">drawing 18</A>
, distribution of encryption contents {data Data} Kc using a computer 140 is
explained.
To a portable telephone 100, a memory card 110 is removable, and the headphone 130
for playing music are connected.
And the portable telephone 100 is connected with the computer 140 through the
telecommunication cable 145.
<BR>[0204]
```

A computer 140 is equipped with a hard disk 141, a controller 142, and an external interface 143.  
And a hard disk 141 is connected with a controller 142 through a bus BS 5, and a controller 142 contains the license protection module 143.  
<BR>[0205]

A hard disk 141 memorizes encryption contents {data Data} Kc distributed to the computer 140 through a bus BS 5 by the Internet distribution.  
If a controller 142 has the Request to Send of encryption contents {data Data} Kc through a telecommunication cable 145 and an external interface 143 from the user of a portable telephone 100, it will output encryption contents {data Data} Kc to the exterior through read-out and an external interface 143 from a hard disk 141.  
<BR>[0206]

An external interface 143 outputs the signal from a controller 142 to the exterior while inputting into a controller 142 the signal inputted into the computer 140 through the telecommunication cable 145 from the portable telephone 100.  
<BR>[0207]

The license protection module 144 has the same configuration as the data-processing section 310 shown in

```
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web.cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000007"
TARGET="tjitemdrw">drawing 5</A>
, exchanging a portable telephone 100 and a memory card 110, a open cryptographic key, a session key, etc., as mentioned above, in order to transmit encryption contents {data Data} Kc to the memory card 110 with which the portable telephone 100 was equipped, protects encryption contents {data Data} Kc, and transmits it to a memory card 110.
<BR>[0208]
```

Encryption contents {data Data} Kc is distributed to a computer 140 by the Internet distribution from a distribution server, and encryption contents data are memorized by the hard disk 141 of a computer 140 through the bus BS 5 by it.  
<BR>[0209]

If the user of a portable telephone 100 inputs a Request to Send from the key stroke section 1108, a Request to Send will be inputted into a controller 142 through a telecommunication cable 145 and an external interface 143. A controller 142 will input demanded encryption contents {data Data} Kc into read-out and the license protection module 144 from a hard disk 141 through a bus BS 5, if a Request to Send is received.  
<BR>[0210]

The license protection module 144 exchanges a open cryptographic key, a session key, etc. through a memory card 110 and a telecommunication cable 145, as mentioned above, and it transmits encryption contents {data Data} Kc to a memory card 110.  
<BR>[0211]

After transmission, by the same approach as having mentioned above, the user of a portable telephone 100 has the license (content ID, the license key Kc, the count limit AC 1 of playback, and playback length AC 2) of encryption contents {data Data} Kc distributed from the distribution server 30, and reproduces encryption contents {data Data} Kc.  
<BR>[0212]

When CD is used, once after recording encryption contents {data Data} Kc which acquired from Music CD and was generated on a hard disk 141, it may transmit to a memory card 110, and may transmit to a memory card 110 directly, without transmitting to a hard disk 141.  
<BR>[0213]

Encryption contents data {Data} As shown in  
<A

```
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web.cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D0000021"
TARGET="tjitemdrw">drawing 19</A>
, Kc may equip a computer 140 with a memory card 110 directly, and may record encryption contents {data Data} Kc on a memory card 110.
In this case, the controller 142 of a computer 140 records encryption contents data on a memory card 110 directly with the license protection module 144.
<BR>[0214]
```

Also in

```

<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web.cgi_ejje?u=http%3A%2F%2Fwww4.ipd
l.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B
%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000021"
TARGET="tjitemdrw">drawing 19</A>
, a computer 140 acquires encryption contents {data Data} Kc by the same approach as
the case where it is shown in
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web.cgi_ejje?u=http%3A%2F%2Fwww4.ipd
l.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B
%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000020"
TARGET="tjitemdrw">drawing 18</A>
<BR>[0215]

```

The portable telephone 100 of the flow chart in the case of performing a distribution demand of the license containing the license key corresponding to encryption contents {data Data} Kc which newly received to the distribution server 30, and the flow chart which reproduces encryption contents {data Data} Kc which newly received is the same as that of

```

<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web.cgi_ejje?u=http%3A%2F%2Fwww4.ipd
l.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B
%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000011"
TARGET="tjitemdrw">drawing 9</A>
-
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web.cgi_ejje?u=http%3A%2F%2Fwww4.ipd
l.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B
%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000014"
TARGET="tjitemdrw">drawing 12</A>
and
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web.cgi_ejje?u=http%3A%2F%2Fwww4.ipd
l.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B
%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000017"
TARGET="tjitemdrw">drawing 15</A>
, and the flow chart shown in 16.
<BR>[0216]

```

Although the count length AC 1 of playback and the playback length AC 2 were explained as the count limit of playback, and playback length, respectively, as long as the count of playback adds a limit to the playback in a data playback terminal, it may perform limit [ which ] that the count length AC 1 of playback should just be control information which adds a limit to the treatment of a license with a recording device.

<BR>[0217]

Moreover, although the portable telephone 100 was explained as a Data Terminal Equipment which receives distribution of encryption contents data or a license, as long as it is especially unnecessary in a call function etc., it merely has the data communication facility which can perform reception of encryption contents data or a license and it can record the received data, you may be what kind of Data Terminal Equipment.

<BR>[0218]

Furthermore, although the portable telephone 100 is equipped with the function which reproduces contents data (music data), as long as it does not necessarily need a data regenerative function, but it merely has the data communication facility which can perform reception of encryption contents data or a license and it can record the received data, you may be what kind of Data Terminal Equipment.

<BR>[0219]

Furthermore, although it explained that encryption contents data or a license was recorded on the memory card which is a removable recording apparatus, it does not limit to a memory card.

And in the gestalt of operation, it is not necessary to be a removable recording device.

<BR>[0220]

According to the gestalt of operation of this invention, if the distribution demand of encryption contents data is inputted from a user, since the record situation of the memory card with which it was equipped will be searched and required encryption contents data, a license key, etc. will be received from a distribution server according to the record situation, encryption contents data, a license key, etc. overlap, and a portable telephone is not recorded on a memory card.

Moreover, it can prevent paying the useless tariff by overlapping and receiving a license to a distribution server.

Furthermore, it can prevent that useless time amount generates encryption contents data by overlapping and receiving.

<BR>[0221]

It should be thought that the gestalt of the operation indicated this time is [ no ] instantiation at points, and restrictive.

The range of this invention is shown by the above-mentioned not explanation but claim of the gestalt of operation, and it is meant that all modification in a claim, equal semantics, and within the limits is included.

<BR><BR>

<BR><BR><HR>DESCRIPTION OF DRAWINGS

<HR>[Brief Description of the Drawings]

<BR><A

HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran\_web.cgi\_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FNO0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000003"  
TARGET="tjitemdrw">[Drawing 1]</A>

It is the schematic diagram which explains a data distribution system notionally.

<BR><A

HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran\_web.cgi\_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FNO0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000004"  
TARGET="tjitemdrw">[Drawing 2]</A>

It is drawing showing properties, such as data for the communication link in the data distribution system shown in

<A

HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran\_web.cgi\_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FNO0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000003"  
TARGET="tjitemdrw">drawing 1</A>

, and information.

<BR><A

HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran\_web.cgi\_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FNO0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000005"  
TARGET="tjitemdrw">[Drawing 3]</A>

It is drawing showing properties, such as data for the communication link in the data distribution system shown in

<A

HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran\_web.cgi\_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FNO0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000003"  
TARGET="tjitemdrw">drawing 1</A>

, and information.

<BR><A  
 HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran\_web.cgi\_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000006"  
 TARGET="tjitemdrw">[Drawing 4]</A>

It is drawing showing properties, such as data for the communication link in the data distribution system shown in

<A  
 HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran\_web.cgi\_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000003"  
 TARGET="tjitemdrw">drawing 1</A>  
 , and information.

<BR><A  
 HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran\_web.cgi\_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000007"  
 TARGET="tjitemdrw">[Drawing 5]</A>

It is the outline block diagram showing the configuration of a license server.

<BR><A  
 HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran\_web.cgi\_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000008"  
 TARGET="tjitemdrw">[Drawing 6]</A>

It is the block diagram showing the configuration of a portable telephone.

<BR><A  
 HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran\_web.cgi\_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000009"  
 TARGET="tjitemdrw">[Drawing 7]</A>

It is the block diagram showing the configuration of a memory card.

<BR><A  
 HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran\_web.cgi\_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000010"  
 TARGET="tjitemdrw">[Drawing 8]</A>

It is a conceptual diagram for explaining the record condition of a memory card.

<BR><A  
 HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran\_web.cgi\_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000011"  
 TARGET="tjitemdrw">[Drawing 9]</A>

It is the 1st flow chart for explaining the distribution actuation in the data distribution system shown in

<A  
 HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran\_web.cgi\_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000003"  
 TARGET="tjitemdrw">drawing 1</A>

<BR><A  
 HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran\_web.cgi\_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000012"  
 TARGET="tjitemdrw">[Drawing 10]</A>



It is the 2nd flow chart for explaining the distribution actuation in the data distribution system shown in

```
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D0000003"
TARGET="tjitemdrw">drawing 1</A>
<BR><A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D0000003"
TARGET="tjitemdrw">[Drawing 11]</A>
```

It is the 3rd flow chart for explaining the distribution actuation in the data distribution system shown in

```
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D0000003"
TARGET="tjitemdrw">drawing 1</A>
<BR><A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D0000003"
TARGET="tjitemdrw">[Drawing 12]</A>
```

It is the 4th flow chart for explaining the distribution actuation in the data distribution system shown in

```
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D0000003"
TARGET="tjitemdrw">drawing 1</A>
<BR><A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D0000003"
TARGET="tjitemdrw">[Drawing 13]</A>
```

It is drawing showing the condition of having displayed the contents menu transmitted to the portable telephone from the distribution server on the display of a portable telephone.

```
<BR><A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D0000003"
TARGET="tjitemdrw">[Drawing 14]</A>
```

It is a data format in the memory of a memory card.

```
<BR><A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D0000003"
TARGET="tjitemdrw">[Drawing 15]</A>
```

It is the 1st flow chart for explaining the playback actuation in a portable telephone.

```
<BR><A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D0000003"
TARGET="tjitemdrw">[Drawing 15]</A>
```

%3F6%3E7%3D8%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000018"  
 TARGET="tjitemdrw">[Drawing 16]</A>

It is the 2nd flow chart for explaining the playback actuation in a portable telephone.

<BR><A  
 HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran\_web.cgi\_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000019"  
 TARGET="tjitemdrw">[Drawing 17]</A>

It is drawing explaining the encryption contents data according to the record situation of a memory card, and the example of distribution of a license.

<BR><A  
 HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran\_web.cgi\_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000020"  
 TARGET="tjitemdrw">[Drawing 18]</A>

It is a schematic diagram for explaining distribution of the encryption contents data using a computer notionally.

<BR><A  
 HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran\_web.cgi\_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2Ftokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000021"  
 TARGET="tjitemdrw">[Drawing 19]</A>

They are other schematic diagrams for explaining distribution of the encryption contents data using a computer notionally.

<BR>[Description of Notations]

<BR>10 License Server, 20 Distribution Carrier, 30 Distribution Server,  
 60 A contents menu, 100 A portable telephone, 110 Memory card,  
 130 A head telephone, 140 A computer, 141 Hard disk,  
 142, 1106, 1420 A controller, 143 External interface,  
 144 License \*\* A \*\* module, 145 Telecommunication cable,  
 302 An accounting database, a 304 information database, 306 CRL database,  
 307 A menu database, 308 Distribution record database,  
 310 The data-processing section, 312, 320, 1206, 1212, 1214, 1404, 1408 and 1412,  
 the 1422 decode processing section,  
 313 An authentication key attaching part, 315 A distribution control section,  
 316, 1210, 1418 Session key generating section,  
 318, 326, 328, 1208, 1406, 1410 Cipher-processing section,  
 350 A communication device, 1102 An antenna, the 1104 transceiver sections,  
 1108 Key stroke section,  
 1110 A display, 1111 The shift section, 1112 Voice playback section,  
 1113 1218 A DA converter, 1114, 1201, 1220, 1224 Terminal,  
 1115 A microphone, 1116 An A-D converter, 1117 Voice coding section,  
 1200 1202 A memory interface, 1400 Authentication data-hold section,  
 1204 Kpl attaching part, 1216 The music playback section, 1222 Switch,  
 1402 Kmc1 attaching part, 1414 A Kpma attaching part, 1415 Memory,  
 1415A CRL field, 1415B A data area, 1416Kpml attaching part, 1421 Kml  
 attaching part, 1423 An interface, 1424 Header, 1440 A license information  
 attaching part, 1442, 1444, 1446 Change-over switch.

<BR><BR>

<HR></BODY></HTML>

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号  
特開2002-91827  
(P2002-91827A)

(43)公開日 平成14年3月29日(2002.3.29)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	テ-コ-ド <sup>*</sup> (参考)	
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 B	5 B 0 1 7
12/00	5 3 7	12/00	5 3 7 H	5 B 0 4 9
17/60	3 0 2	17/60	3 0 2 E	5 B 0 8 2

審査請求 未請求 請求項の数14 O L (全 31 頁)

(21)出願番号 特願2000-284862(P2000-284862)

(22)出願日 平成12年9月20日(2000.9.20)

(71)出願人 000001889

三洋電機株式会社

大阪府守口市京阪本通2丁目5番5号

(72)発明者 堀 吉宏

大阪府守口市京阪本通2丁目5番5号 三  
洋電機株式会社内

(74)代理人 100064746

弁理士 深見 久郎 (外3名)

Fターム(参考) 5B017 AA07 BA07 EB07 CA16

5B049 AA05 AA06 EB05 FF01 FF08

GG00

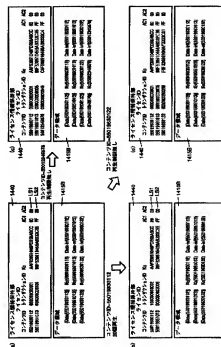
5B082 GA11

(54)【発明の名称】 データ端末装置

(57)【要約】

【課題】 必要な暗号化コンテンツデータおよび/またはライセンス鍵等のみを配信サーバから受信する携帯端末装置を提供する。

【解決手段】 携帯電話機は、ユーザから暗号化コンテンツデータ [Data] Kcの受信要求が入力されると、装着されたメモリカードにおけるコンテンツID、ライセンス鍵Kc、再生回数制限情報AC1、再生期限、および暗号化コンテンツデータ [Data] Kc等の記録状況を検索する。そして、メモリカードのライセンス領域1415A、データ領域1415Bに記録されていない暗号化コンテンツデータ [Data] Kc、およびライセンス (コンテンツID、ライセンス鍵Kc、再生回数制限情報AC1、再生期限) だけを配信サーバから受信する。



## 【特許請求の範囲】

【請求項1】 コンテンツデータを暗号化した暗号化コンテンツデータおよび/または前記暗号化コンテンツデータを再生するためのライセンスを配信サーバから受信して、前記暗号化コンテンツデータおよび/または前記ライセンスを記録するデータ端末装置であって、前記暗号化コンテンツデータおよび前記ライセンスを記録するデータ記録部と、

外部との通信を行なう送受信部と、前記データ記録部とのデータ授受を制御するインタフェースと、

指示を入力するためのキー操作部と、

制御部とを備え、

前記制御部は、前記キー操作部を介して暗号化コンテンツデータの受信要求が入力されると、受信要求された暗号化コンテンツデータが前記データ記録装置に記録されているかを検索し、かつ、受信要求された暗号化コンテンツデータを再生することができるライセンスの有無を検索し、

前記暗号化コンテンツデータが前記データ記録部に記録されていないとき、および/または前記ライセンスが無いとき、前記暗号化コンテンツデータおよび/または前記ライセンスの配信を前記送受信部を介して配信サーバへ要求する、データ端末装置。

【請求項2】 前記制御部は、前記送受信部が前記配信サーバから受信した暗号化コンテンツデータのメニュー情報に基づいて、受信要求する暗号化コンテンツデータが決定された後に、前記暗号化コンテンツデータおよび/または前記ライセンスの検索を行なう、請求項1に記載のデータ端末装置。

【請求項3】 前記受信要求する暗号化コンテンツデータの決定は、前記メニュー情報に含まれた暗号化コンテンツデータを特定するためのコンテンツIDが選択されることによって行なわれ、

前記制御部は、前記選択されたコンテンツIDに基づいて前記暗号化コンテンツデータおよび/または前記ライセンスの検索を行なう、請求項2に記載のデータ端末装置。

【請求項4】 前記制御部は、前記暗号化コンテンツデータの検索を行ない、前記暗号化コンテンツデータが前記データ記録部に記録されていないとき、前記暗号化コンテンツデータの配信を前記送受信部を介して前記配信サーバへ要求する、請求項1から請求項3のいずれか1項に記載のデータ端末装置。

【請求項5】 前記制御部は、前記暗号化コンテンツデータが前記データ記録装置に記録されているとき、前記ライセンスの検索を行なう、請求項4に記載のデータ端末装置。

【請求項6】 前記ライセンスは、少なくとも前記暗号化コンテンツデータを復号するためのライセンス鍵と、

前記暗号化コンテンツデータの再生を制限する再生制限情報とから成り、

前記制御部は、受信要求された暗号化コンテンツデータが前記データ記録部に記録されており、前記ライセンス鍵および前記再生制限情報が前記データ記録部に記録されていないとき、前記ライセンスが無いと判断する、請求項1に記載のデータ端末装置。

【請求項7】 前記ライセンスは、少なくとも前記暗号化コンテンツデータを復号するためのライセンス鍵と、前記暗号化コンテンツデータの再生を制限する再生制限情報とから成り、

前記制御部は、受信要求された暗号化コンテンツデータおよびその暗号化コンテンツデータを復号するためのライセンス鍵が前記データ記録部に記録されており、前記暗号化コンテンツデータの再生が前記再生制限情報によって制限されているとき、前記ライセンスが無いと判断する、請求項1に記載のデータ端末装置。

【請求項8】 前記制御部は、前記キー操作部から入力された変更後の再生制限情報を前記ライセンスの購入条件として前記コンテンツIDとともに前記送受信部を介して前記配信サーバへ送信する、請求項7に記載のデータ端末装置。

【請求項9】 表示部をさらに備え、

前記制御部は、前記メニュー情報を前記表示部に表示し、ユーザが前記表示部に表示された前記メニュー情報に基づいて前記コンテンツIDを選択するための情報をキー操作部を介して入力することによって、前記コンテンツIDを取得する、請求項3に記載のデータ端末装置。

【請求項10】 前記メニュー情報は、他の画面へ移行するための移行情報を含む複数の画面から構成され、前記表示部は、前記移行情報を入力するための入力部を含み、

前記制御部は、前記入力部から前記移行情報が入力されると、前記移行情報に基づいて決定される他の画面を前記表示部に表示する、請求項9に記載のデータ端末装置。

【請求項11】 前記制御部は、前記ライセンスの購入条件と、前記インタフェースを介して取得した前記データ記録部の認証データおよび前記コンテンツIDとを前記送受信部を介して前記配信サーバへ送信し、前記配信サーバにおいて前記認証データが認証された場合のみ、前記ライセンスを受信する、請求項1から請求項10のいずれか1項に記載のデータ端末装置。

【請求項12】 前記ライセンスに従って前記暗号化コンテンツデータを再生するデータ再生部をさらに備え、前記制御部は、前記キー操作部を介して暗号化コンテンツデータの再生要求が入力されると、前記暗号化コンテンツデータに対する前記ライセンスのうち少なくとも前記データ再生部に必要な情報と前記暗号化コンテンツ

ータとを前記データ記録部から前記インタフェースを介して受取り、その受取った暗号化コンテンツデータおよび前記必要な情報を前記データ再生部に与える。請求項1から請求項11のいずれか1項に記載のデータ端末装置。

【請求項13】 前記バスに接続され、前記データ記録部に対する認証データを保持する認証データ保持部をさらに備え、

暗号化コンテンツデータの再生時、前記制御部は、前記認証データが前記データ記録部において認証された場合の前記暗号化コンテンツデータに対する前記ライセンスのうち少なくとも前記データ再生部に必要な情報を前記データ記録部から前記インタフェースを介して受取り、その受取った暗号化コンテンツデータおよび前記必要な情報を前記データ再生部に与える。請求項12に記載のデータ端末装置。

【請求項14】 前記データ記録部は、着脱可能なデータ記録装置である。請求項1から請求項13のいずれか1項に記載のデータ端末装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、コピーされた情報に対する著作権保護を可能とするデータ配信システムにおいて用いられるデータ端末装置に関するものである。

【0002】

【従来の技術】近年、インターネット等の情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

【0003】このような情報通信網においては、デジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

【0004】したがって、このような情報通信網において音楽データや画像データ等の著作権者の権利が存在する創作物が伝送される場合、適切な著作権保護のための方法が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

【0005】一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介して著作物データの配信を行なうことができないとすると、基本的には、著作物データの複製に際し一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

【0006】ここで、上述のようなデジタル情報通信網を介した配信ではなく、デジタルデータを記録した記録媒体を例にとりて考えて見ると、通常販売されている音楽データを記録したCD（コンパクトディスク）につい

ては、CDから光磁気ディスク（MD等）への音楽データのコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行なう個人ユーザは、デジタル録音機器自体やMD等の媒体の代金のうちの一定額を間接的に著作権者に対して保証金として支払うことになっている。

【0007】しかも、CDからMDへデジタル信号である音楽データをコピーした場合、これらの情報がコピー劣化の殆どないデジタルデータであることに鑑み、記録可能なMDからさらに他のMDに音楽情報をデジタルデータとしてコピーすることは、著作権保護のために機器の構成上できないようになっている。

【0008】このような事情からも、音楽データや画像データをデジタル情報通信網を通じて公衆に配信を受けることは、それ自身が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方法が講じられる必要がある。

【0009】この場合、情報通信網を通じて公衆に送信される著作物である音楽データや画像データ等のコンテンツデータについて、一度受信されたコンテンツデータが、さらに勝手に複製されることを防止することが必要となる。

【0010】そこで、コンテンツデータを暗号化した暗号化コンテンツデータを保持する配信サーバが、携帯電話機等の端末装置に装着されたメモリカードに対して端末装置を介して暗号化コンテンツデータを配信するデータ配信システムが提案されている。このデータ配信システムにおいては、予め認証局で認証されたメモリカードの公開暗号鍵とその証明書書を暗号化コンテンツデータの配信要求の際に配信サーバへ送信し、配信サーバが認証された証明書書を受信したことを確認した上でメモリカードに対して暗号化コンテンツデータと、暗号化コンテンツデータを復号するためのライセンス鍵を送信する。そして、暗号化コンテンツデータやライセンス鍵を配信する際、配信サーバおよびメモリカードは、配信毎に異なるセッションキーを発生させ、その発生させたセッションキーによって公開暗号鍵の暗号化を行ない、配信サーバ、メモリカード相互間で鍵の交換を行なう。

【0011】最終的に、配信サーバは、メモリカード個々の公開暗号鍵によって暗号化され、さらにセッションキーによって暗号化したライセンスと、暗号化コンテンツデータをメモリカードに送信する。そして、メモリカードは、受信したライセンス鍵と暗号化コンテンツデータをメモリカードに記録する。

【0012】そして、メモリカードに記録した暗号化コンテンツデータを再生するときは、メモリカードを携帯電話に装着する。携帯電話は、通常の電話機能の他にメモリカードからの暗号化コンテンツデータを復号し、かつ、再生して外部へ出力するための専用回路も有する。

【0013】このように、携帯電話機のユーザは、携帯電話機を用いて暗号化コンテンツデータを配信サーバから受信し、その暗号化コンテンツデータを再生することができる。

【0014】

【発明が解決しようとする課題】しかし、暗号化コンテンツデータを配信サーバから受信するとき、携帯電話機は、暗号化コンテンツデータとともに暗号化コンテンツデータを復号するライセンス鍵、および暗号化コンテンツデータの再生回数、再生期限等を設定した購入条件を配信サーバから受信し、メモリカードに記録する。

【0015】また、携帯電話機は、暗号化コンテンツデータを再生するとき、暗号化コンテンツデータの再生が受信した再生回数、再生期限等によって制限されないときに暗号化コンテンツデータを再生する。

【0016】さらに、携帯電話機は、配信サーバ以外から暗号化コンテンツデータのみを受信し、メモリカードに記録する場合もある。

【0017】したがって、暗号化コンテンツデータがメモリカードに記録されているが、ライセンス鍵がメモリカードに記録されていない場合、暗号化コンテンツデータおよびライセンス鍵がメモリカードに記録されているが、再生回数、再生期限等によって暗号化コンテンツデータの再生が制限される場合、および暗号化コンテンツデータおよびライセンス鍵がメモリカードに記録されていない場合等が想定される。

【0018】かかる場合に、ユーザから暗号化コンテンツデータの配信要求がされた場合、直ちに配信サーバへ暗号化コンテンツデータおよびライセンス鍵等の配信を要求したのでは、同じ暗号化コンテンツデータおよびライセンス鍵を配信サーバから受信することになり、同じ暗号化コンテンツデータに対して料金を複数回支払うという問題が生じる。

【0019】また、暗号化コンテンツデータを配信サーバから受信するために不要な時間を必要とするという問題もある。

【0020】そこで、本発明は、かかる問題を解決するためのになされたものであり、その目的は、必要な暗号化コンテンツデータおよび/またはライセンス鍵等のみを配信サーバから受信するデータ端末装置を提供することである。

【0021】

【課題を解決するための手段および発明の効果】この発明によるデータ端末装置は、コンテンツデータを暗号化した暗号化コンテンツデータおよび/または暗号化コンテンツデータを再生するためのライセンスを配信サーバから受信して、暗号化コンテンツデータおよび/またはライセンスを記録するデータ端末装置であって、暗号化コンテンツデータおよびライセンスを記録するデータ記録部と、外部との通信を行なう送受信部と、データ記録

部とのデータ授受を制御するインタフェースと、指示を入力するためのキー操作部と、制御部とを備え、制御部は、キー操作部を介して暗号化コンテンツデータの受信要求が入力されると、受信要求された暗号化コンテンツデータがデータ記録部に記録されているかを検索し、かつ、受信要求された暗号化コンテンツデータを再生するためのライセンスの有無を検索し、暗号化コンテンツデータがデータ記録部に記録されていないとき、および/またはライセンスが無いとき、暗号化コンテンツデータおよび/またはライセンスの配信を送受信部を介して配信サーバへ要求する。

【0022】この発明によるデータ端末装置においては、ユーザから暗号化コンテンツデータの受信要求がキー操作部を介して入力されると、制御部は、受信要求がなされた暗号化コンテンツデータおよび/またはライセンスがデータ記録部に記録されているか否かを検索し、データ記録部に記録されていない暗号化コンテンツデータおよび/またはライセンスの配信を配信サーバへ要求する。つまり、データ端末装置は、データ記録部における暗号化コンテンツデータおよびライセンスの記録状況に応じて必要な暗号化コンテンツデータおよびライセンスだけを配信サーバから受信し、かつ、データ記録部に記録する。

【0023】したがって、この発明によれば、データ記録部における暗号化コンテンツデータおよびライセンスの重複記録を防止できる。

【0024】また、この発明によれば、ライセンスを重複して受信することによる無駄な料金を配信サーバへ支払うことを防止できる。

【0025】さらに、この発明によれば、暗号化コンテンツデータを重複して受信することによって無駄な時間が発生するのを防止できる。

【0026】好ましくは、データ端末装置の制御部は、送受信部が配信サーバから受信した暗号化コンテンツデータのメニュー情報に基づいて、受信要求する暗号化コンテンツデータが決定された後に、暗号化コンテンツデータおよび/またはライセンスの検索を行なう。

【0027】データ端末装置は、配信サーバから受信したメニュー情報に基づいて、受信要求する暗号化コンテンツデータが決定された後に暗号化コンテンツデータおよび/またはライセンスの検索を行なう。

【0028】したがって、この発明によれば、受信要求された暗号化コンテンツデータおよびライセンスがデータ記録部に記録されているか否かを正確に判断できる。

【0029】好ましくは、受信要求する暗号化コンテンツデータの決定は、メニュー情報に含まれた暗号化コンテンツデータを特定するためのコンテンツIDが選択されることによって行なわれ、制御部は、選択されたコンテンツIDに基づいて暗号化コンテンツデータおよび/またはライセンスの検索を行なう。

【0030】ユーザは、暗号化コンテンツデータのコンテンツIDを特定することによって受信要求する暗号化コンテンツデータを選択する。そうすると、データ端末装置の制御部は、選択された暗号化コンテンツデータのコンテンツIDを抽出し、その抽出したコンテンツIDに基づいて、暗号化コンテンツデータおよび/またはライセンスがデータ記録部に記録されているか否かを検索する。

【0031】したがって、この発明によれば、データ記録部における暗号化コンテンツデータおよび/またはライセンスの検索を正確に行うことができる。

【0032】好ましくは、データ端末装置の制御部は、暗号化コンテンツデータの検索を行ない、暗号化コンテンツデータがデータ記録部に記録されていないとき、暗号化コンテンツデータの配信を送受信部を介して配信サーバへ要求する。

【0033】データ端末装置の制御部は、コンテンツIDを用いてデータ記録部における暗号化コンテンツデータの検索を行ない、暗号化コンテンツデータがデータ記録部に記録されていないとき、データ記録部におけるライセンスの検索を行わずに暗号化コンテンツデータおよびライセンスの配信を配信サーバへ要求する。

【0034】したがって、この発明によれば、データ記録部における暗号化コンテンツデータおよびライセンスの記録状況を迅速に検索し、その記録状況に応じて必要な暗号化コンテンツデータおよびライセンスを配信サーバから受信できる。

【0035】好ましくは、データ端末装置の制御部は、暗号化コンテンツデータがデータ記録部に記録されているとき、ライセンスの検索を行なう。

【0036】データ端末装置の制御部は、暗号化コンテンツデータがデータ記録部に記録されていないことを確認した後、ライセンスの検索を行なう。

【0037】したがって、この発明によれば、必要な検索のみを行なうことによって検索時間を短縮し、かつ、正確な検索を行なうことができる。

【0038】好ましくは、ライセンスは、少なくとも暗号化コンテンツデータを復号するためのライセンス鍵と、暗号化コンテンツデータの再生を制限する再生制限情報とから成り、制御部は、受信要求された暗号化コンテンツデータがデータ記録部に記録されており、ライセンス鍵および再生制限情報がデータ記録部に記録されていないとき、ライセンスが無いと判断する。

【0039】ライセンスを構成するライセンス鍵および再生制限情報がデータ記録部に記録されていないとき、データ端末装置の制御部は、受信要求された暗号化コンテンツデータのライセンスが存在しないと判断する。

【0040】したがって、この発明によれば、データ記録部に暗号化コンテンツデータのみが記録されているとき、ライセンス鍵および再生制限情報を配信サーバから

受信することができる。

【0041】好ましくは、ライセンスは、少なくとも暗号化コンテンツデータを復号するためのライセンス鍵と、暗号化コンテンツデータの再生を制限する再生制限情報とから成り、制御部は、受信要求された暗号化コンテンツデータおよびその暗号化コンテンツデータを復号するためのライセンス鍵がデータ記録部に記録されており、暗号化コンテンツデータの再生が再生制限情報によって制限されているとき、ライセンスが無いと判断する。

【0042】ライセンスを構成する再生制限情報のみがデータ記録部に記録されていないとき、データ端末装置の制御部は、受信要求された暗号化コンテンツデータのライセンスが存在しないと判断する。

【0043】したがって、この発明によれば、再生制限情報のみがデータ記録部に記録されていないとき、再生制限情報を配信サーバから受信してライセンスを取得することができる。

【0044】好ましくは、データ端末装置の制御部は、キー操作部から入力された変更後の再生制限情報をライセンスの購入条件としてコンテンツIDとともに送受信部を介して配信サーバへ送信する。

【0045】データ端末装置の制御部は、再生制限情報のみを変更することによって暗号化コンテンツデータの購入条件が設定されると、コンテンツIDとともに設定された購入条件を配信サーバへ送信する。そして、データ端末装置は、再生制限情報を配信サーバから受信し、データ記録部に記録する。

【0046】したがって、この発明によれば、ライセンスを購入して暗号化コンテンツデータを再生し、ライセンスが無くなった場合にも新たに再生制限情報だけを配信サーバから購入することによって暗号化コンテンツデータを再生することができる。

【0047】好ましくは、データ端末装置は、表示部をさらに備え、制御部は、メニュー情報を表示部に表示し、ユーザが表示部に表示されたメニュー情報に基づいてコンテンツIDを選択するための情報をキー操作部を介して入力することによって、コンテンツIDを取得する。

【0048】配信サーバから配信されたメニュー情報は、データ端末装置の表示部に表示される。そして、ユーザは表示部に表示されたメニュー情報を見て受信を希望する暗号化コンテンツデータのコンテンツIDを選択するための情報をキー操作部から入力する。そうすると制御部は、キー操作部を介して選択されたコンテンツIDを取得する。

【0049】したがって、この発明によれば、ユーザは視覚情報に基づいて受信を希望する暗号化コンテンツデータを決定できる。また、この発明によれば、コンテンツIDを選択するための情報が入力されるので、制御部

は、選択されたコンテンツIDに基づいて、暗号化コンテンツデータおよび/またはライセンスの検索を迅速に行うことができる。

【0050】好ましくは、メニュー情報は、他の画面へ移行するための移行情報を含む複数の画面から構成され、表示部は、移行情報を入力するための入力部を含み、制御部は、入力部から移行情報が入力されると、移行情報に基づいて決定される他の画面を表示部に表示する。

【0051】データ端末装置の表示部に表示されたメニュー情報に受信を希望する暗号化コンテンツデータが含まれていないとき、ユーザは移行情報を入力する。そうすると、データ端末装置の制御部は、次の画面に移行し、新たなメニュー情報を表示部に表示する。

【0052】したがって、この発明によれば、多くの暗号化コンテンツデータの中から受信を希望する暗号化コンテンツデータを選択できる。

【0053】好ましくは、データ端末装置の制御部は、ライセンスの購入条件と、インタフェースを介して取得したデータ記録部の認証データおよびコンテンツIDとを送受信部を介して配信サーバへ送信し、配信サーバにおいて認証データが認証された場合のみ、ライセンスを受信する。

【0054】配信サーバがデータ記録部から送られてきた認証データを認証した場合のみ、データ端末装置はライセンスを受信する。

【0055】したがって、この発明によれば、正規なデータ記録部にだけライセンスを与えることができる。その結果、暗号化コンテンツデータの保護を図ることができる。

【0056】好ましくは、データ端末装置は、ライセンスに従って暗号化コンテンツデータを再生するデータ再生部をさらに備え、制御部は、キー操作部を介して暗号化コンテンツデータの再生要求が入力されると、暗号化コンテンツデータに対するライセンスのうち少なくともデータ再生部に必要な情報と暗号化コンテンツデータとをデータ記録部からインタフェースを介して受取り、その受取った暗号化コンテンツデータおよび必要な情報をデータ再生部に与える。

【0057】暗号化コンテンツデータの再生時、制御部は、ライセンスを構成する種々の情報のうち、再生に必要な情報だけをデータ記録部から取出し、暗号化コンテンツデータと、再生に必要な情報とをデータ再生部に与える。そして、データ再生部は、必要な情報によって暗号化コンテンツデータを復号および再生する。

【0058】したがって、この発明によれば、再生に必要な情報によって暗号化コンテンツデータの再生を制限することができる。

【0059】好ましくは、データ端末装置は、データ記録部に対する認証データを保持する認証データ保持部を

さらに備え、暗号化コンテンツデータの再生時、制御部は、認証データがデータ記録部において認証された場合のみ暗号化コンテンツデータに対するライセンスのうち少なくともデータ再生部に必要な情報をデータ記録部からインタフェースを介して受取り、その受取った暗号化コンテンツデータをデータ再生部に与える。

【0060】配信サーバから受信した暗号化コンテンツデータを再生するとき、データ記録部に対するデータ端末装置の正当性が確認された場合だけ、データ端末装置はデータ記録部から暗号化コンテンツデータを受取り、暗号化コンテンツデータを再生する。

【0061】したがって、この発明によれば、正規なデータ端末装置だけが暗号化コンテンツデータを再生できる。その結果、暗号化コンテンツデータの不法なコピー等を防止して保護を図ることができる。

【0062】好ましくは、データ記録部は、データ端末装置から着脱可能なデータ記録装置である。

【0063】データ端末装置は、配信サーバから暗号化コンテンツデータおよびライセンスを受信すると、その受信した暗号化コンテンツデータおよびライセンスを着脱可能なデータ記録装置へに記録する。

【0064】したがって、この発明によれば、複数のデータ記録装置に暗号化コンテンツデータおよび/またはライセンスを記録することができる。

【0065】

【発明の実施の形態】本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

【0066】図1は、本発明による携帯端末装置が再生の対象とする暗号化コンテンツデータをメモリカードへ配信するデータ配信システムの全体構成を概念的に説明するための概略図である。

【0067】なお、以下では携帯電話機網を介してデジタル音楽データを各携帯電話ユーザに配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物としてのコンテンツデータ、たとえば画像データ、動画像データ等を配信する場合においても適用することが可能なものである。

【0068】図1を参照して、配信キャリア20は、自己の携帯電話網を通じて得た、各携帯電話ユーザからの配信要求(配信リクエスト)をライセンスサーバ10に中継する。著作権の存在する音楽データを管理するライセンスサーバ10は、データ配信を求めてアクセスして来た携帯電話ユーザの携帯電話機100に装着されたメモリカード110が正当な認証データを持つか否か、すなわち、正規のメモリカードであるか否かの認証処理を行い、正当なメモリカードに対して所定の暗号方式により音楽データ(以下コンテンツデータとも呼ぶ)を暗号化した上で、データを配信するための配信キャリア20で



ある携帯電話会社に、このような暗号化コンテンツデータおよび暗号化コンテンツデータを再生するために必要な情報としてライセンスを与える。

【0069】配信キャリア20は、自己の携帯電話網を通じて配信要求を送信した携帯電話機100に装着されたメモリカード110に対して、携帯電話網および携帯電話機100を介して暗号化コンテンツデータとライセンスとを配信する。

【0070】図1においては、たとえば携帯電話ユーザの携帯電話機100には、着脱可能なメモリカード110が装着される構成となっている。メモリカード110は、携帯電話機100により受信された暗号化コンテンツデータを受取り、上記配信にあたって行なわれた暗号化を復号した上で、携帯電話機100中の音楽再生部（図示せず）に与える。

【0071】さらに、たとえば携帯電話ユーザは、携帯電話機100に接続したヘッドホン130等を介してこのようなコンテンツデータを「再生」して、聴取することが可能である。

【0072】以下では、このようなライセンスサーバ10と配信キャリア20と併せて、配信サーバ30と総称することとする。

【0073】また、このような配信サーバ30から、各携帯電話機等にコンテンツデータを伝送する処理を「配信」と称することとする。

【0074】このように構成とすることで、まず、メモリカード110を利用しないと、配信サーバ30からコンテンツデータの配信を受けて、音楽を再生することが困難な構成となる。

【0075】しかも、配信キャリア20において、たとえば1曲分のコンテンツデータを配信するたびにその度数を計数しておくことで、携帯電話ユーザがコンテンツデータを受信（ダウンロード）するたびに発生する著作権料を、配信キャリア20が携帯電話機の通話料とともに徴収することとすれば、著作権者が著作権料を確保することが容易となる。

【0076】図1に示したような構成においては、暗号化して配信されるコンテンツデータを携帯電話のユーザ側で再生可能とするためにシステム上必要とされるのは、第1には、通信における暗号鍵を配信するための方式であり、さらに第2には、配信したいコンテンツデータを暗号化する方式そのものであり、さらに、第3には、このように配信されたコンテンツデータの無断コピーを防止するためのコンテンツデータ保護を実現する構成である。

【0077】本発明の実施の形態においては、特に、配信、および再生の各セッションの発生時において、これらのコンテンツデータの移動先に対する認証およびチェック機能を充実させ、非認証もしくは復号鍵の破られた記録装置およびデータ再生端末（コンテンツを再生でき

るデータ再生端末を携帯電話機とも言う。以下同じ）に対するコンテンツデータの出力を防止することによってコンテンツデータの著作権保護を強化する構成を説明する。

【0078】図2は、図1に示したデータ配信システムにおいて、使用される通信のためのデータ、情報等の特性を説明する図である。

【0079】まず、配信サーバ30より配信されるデータについて説明する。Dataは、音楽データ等のコンテンツデータである。コンテンツデータDataには、ライセンス鍵Kcで復号可能な暗号化が施される。ライセンス鍵Kcによって復号可能な暗号化が施された暗号化コンテンツデータ [Data] Kcがこの形式で配信サーバ30より携帯電話ユーザに配布される。

【0080】なお、以下においては、[Y] Xという表記は、データYを、復号鍵Xにより復号可能な暗号化を施したことを示すものとする。

【0081】さらに、配信サーバ30からは、暗号化コンテンツデータとともに、コンテンツデータに関する著作権あるいはサーバアクセス関連等の平文情報としての付加情報Data in fが配布される。また、配信サーバ30からの暗号化コンテンツデータおよびライセンス鍵等の配信を特定するための管理コードであるトランザクションIDが配信サーバ30と携帯電話機100との間でやり取りされる。さらに、ライセンス情報としては、コンテンツデータDataを識別するためのコードであるコンテンツIDおよびライセンスの発行を特定できる管理コードであるライセンスIDや、利用者側からの指定によって決定されるライセンス数や機能限定等の情報を含んだライセンス購入条件ACに基づいて生成される、記録装置（メモリカード）のアクセスに対する制限に関する情報であるアクセス制限情報AC1およびデータ再生端末における制御情報である再生期限AC2等が存在する。以後、ライセンス鍵KcとコンテンツIDとライセンスIDと再生回数期限AC1と再生期限AC2とを併せて、ライセンスと総称することとする。

【0082】図3は、図1に示すデータ配信システムにおいて使用される認証および禁止クラスリストの運用のためのデータ、情報等の特性を説明する図である。

【0083】本発明の実施の形態においては、記録装置（メモリカード）やコンテンツデータを再生する携帯電話機のクラスごとに、コンテンツデータの配信、および再生を禁止することができるように禁止クラスリストCRL (Class Revocation List) の運用を行なう。以下では、必要に応じて記号CRLによって禁止クラスリスト内のデータを表わすこともある。

【0084】禁止クラスリスト関連情報には、ライセンスの配信、および再生が禁止される携帯電話機およびメモリカードのクラスをリストアップした禁止クラスリス

トデータCRLが含まれる。

【0085】禁止クラスリストデータCRLは、配信サーバ30内で管理されるとともに、メモ리카ード内にも記録保持される。このような禁止クラスリストは、随時バージョンアップしデータを更新していく必要があるが、データの変更については、基本的には暗号化コンテンツデータおよび/またはライセンス鍵等のライセンスを配信する際の日時を基準として、携帯電話機から受取った禁止クラスリストの更新の有無を判断し、更新されていないとき、更新された禁止クラスリストを携帯電話機に配信する。また、禁止クラスリストの変更については、変更点のみを反映した差分データCRL<sub>dat</sub>を配信サーバ30側より発生して、これに応じてメモ리카ード内の禁止クラスリストCRLが書き換えられる構成とするも可能である。また、禁止クラスリストのバージョンについては、CRL<sub>ver</sub>をメモ리카ード側より出力し、これを配信サーバ30側で確認することによってバージョン管理を実行する。差分データCRL<sub>dat</sub>には新たなバージョンの情報も含まれる。

【0086】このように、禁止クラスリストCRLを、配信サーバのみならずメモ리카ード内においても保持運用することによって、クラス固有すなわち、携帯電話機およびメモ리카ードの種類に固有の番号鍵が破られた、携帯電話機およびメモ리카ードへのライセンス鍵の供給を禁止する。このため、携帯電話機ではコンテンツデータの再生が、メモ리카ードではコンテンツデータの移動が行えなくなる。

【0087】このように、メモ리카ード内の禁止クラスリストCRLは配信時に逐次データを更新する構成とする。また、メモ리카ード内における禁止クラスリストCRLの管理は、上位レベルとは独立にメモ리카ード内でタンパーレジスタンスモジュール(Tamper Resistance Module)に記録する等によって、ファイルシステムやアプリケーションプログラム等によって上位レベルから禁止クラスリストデータCRLを改ざんすることが不可能な構成とする。この結果、データに関する著作権保護をより強固なものとすることができる。

【0088】携帯電話機およびメモ리카ードには固有の公開暗号鍵K<sub>pn</sub>およびK<sub>pmc</sub>がそれぞれ設けられ、公開暗号鍵K<sub>pn</sub>およびK<sub>pmc</sub>は携帯電話機に固有の秘密復号鍵K<sub>pn</sub>およびメモ리카ード固有の秘密復号鍵K<sub>mc</sub>によってそれぞれ復号可能である。これら公開暗号鍵および秘密復号鍵は、携帯電話機の種類ごとおよびメモ리카ードの種類ごとに異なる値を持つ。これらの公開暗号鍵および秘密復号鍵を総称してクラス鍵と称する。

【0089】また、データ再生端末(携帯電話機)およびメモ리카ードのクラス証明書として、C<sub>rt</sub>f<sub>n</sub>およびC<sub>mc</sub>iがそれぞれ設けられる。これらのクラス証

書は、メモ리카ードおよびコンテンツ再生端末のクラスごとに異なる情報を有する。クラス鍵による暗号が破られた、すなわち、秘密復号鍵が取得されたクラス鍵に対しては、禁止クラスリストにリストアップされてライセンス発行の禁止対象となる。

【0090】この間のメモ리카ードおよびコンテンツ再生端末固有の公開暗号鍵およびクラス証明書は、認証データ[K<sub>pmc</sub>i/C<sub>mc</sub>i]K<sub>pm</sub>aおよび[K<sub>pn</sub>/C<sub>rt</sub>f<sub>n</sub>]K<sub>pm</sub>aの形式で、出荷時にメモ리카ードおよびデータ再生端末(携帯電話機)にそれぞれ記録される。後ほど詳細に説明するが、K<sub>pm</sub>aは配信システム全体で共通の公開認証鍵である。

【0091】図4は、図1に示したデータ配信システムにおいて暗号化に関わる鍵の特性をまとめて説明する図である。

【0092】メモ리카ード外とメモ리카ード間でのデータ授受における秘密保持のための暗号鍵として、コンテンツデータの配信、および再生が行なわれるごとに配信サーバ30、携帯電話機100、メモ리카ード110において生成される共通鍵K<sub>s1</sub>~K<sub>s3</sub>が用いられる。

【0093】ここで、共通鍵K<sub>s1</sub>~K<sub>s3</sub>は、配信サーバ、携帯電話機もしくはメモ리카ード間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵であり、以下においてはこれらの共通鍵K<sub>s1</sub>~K<sub>s3</sub>を「セッションキー」とも呼ぶこととする。

【0094】これらのセッションキーK<sub>s1</sub>~K<sub>s3</sub>は、各通信セッションごとに固有の値を有することにより、配信サーバ、携帯電話機およびメモ리카ードによって管理される。具体的には、セッションキーK<sub>s1</sub>は、配信サーバによって配信セッションごとに発生される。セッションキーK<sub>s2</sub>は、メモ리카ードによって配信セッションおよび再生セッションごとに発生し、セッションキーK<sub>s3</sub>は、携帯電話機において再生セッションごとに発生される。各セッションにおいて、これらのセッションキーを授受し、他の機器で生成されたセッションキーを受けて、このセッションキーによる暗号化を実行したうえでライセンス鍵等の送信を行うことによって、セッションにおけるセキュリティ強度を向上させることができる。

【0095】また、メモ리카ード110内のデータ処理を管理するための鍵として、メモ리카ードという媒体ごとに設定される公開暗号鍵K<sub>pm</sub>と、公開暗号鍵K<sub>pm</sub>で暗号化されたデータを復号することが可能なメモ리카ードごとに固有の秘密復号鍵K<sub>m</sub>が存在する。

【0096】図5は、図1に示したライセンスサーバ100の構成を示す概略ブロック図である。

【0097】ライセンスサーバ10は、コンテンツデータを所定の方式に従って暗号化したデータや、ライセンスID等の配信情報を保持するための情報データベース

304と、各携帯電話ユーザごとにコンテンツデータへのアクセス開始に従った課金情報を保持するための課金データベース302と、禁止クラスリストCRLを管理するCRLデータベース306と、情報データベースに保持されたコンテンツデータのメニューを保持するメニューデータベース307と、コンテンツデータおよびライセンス鍵等の配信を特定するトランザクションIDを保持する配信記録データベース308と、情報データベース304、課金データベース302、CRLデータベース306、メニューデータベース307、および配信記録データベース308からのデータをバスBS1を介して受取り、所定の処理を行なうためのデータ処理部310と、通信網を介して、配信キャリア20とデータ処理部310との間でデータ授受を行なうための通信装置350とを備える。

【0098】データ処理部310は、バスBS1上のデータに応じて、データ処理部310の動作を制御するための配信制御部315と、配信制御部315に制御されて、配信セッション時にセッションキーKs1を発生するためのセッションキー発生部316と、メモリカードおよび携帯電話機から送られてきた認証のための認証データ[KPmc1//Cmc1]KPmaを復号するための公開認証鍵を保持する認証鍵保持部313と、メモリカードおよび携帯電話機から送られてきた認証のための認証データ[KPmc1//Cmc1]KPmaを通信装置350およびバスBS1を介して受けて、認証鍵保持部313からの公開認証鍵KPmaによって復号処理を行なう復号処理部312と、セッションキー発生部316より生成されたセッションキーKs1を復号処理部312によって得られた公開暗号鍵KPmc1を用いて暗号化して、バスBS1に出力するための暗号化処理部318と、セッションキーKs1によって暗号化された上で送信されたデータをバスBS1より受けて、復号処理を行なう復号処理部320とを含む。

【0099】データ処理部310は、さらに、配信制御部315から与えられるライセンス鍵Kcおよび再生期限AC2を、復号処理部320によって得られたメモリカード固有の公開暗号鍵KPmiによって暗号化するための暗号化処理部326と、暗号化処理部326の出力を、復号処理部320から与えられるセッションキーKs2によってさらに暗号化してバスBS1に出力するための暗号化処理部328とを含む。

【0100】ライセンスサーバ10の配信セッションにおける動作については、後ほどフローチャートを用いて詳細に説明する。

【0101】図6は、図1に示した携帯電話機100の構成を説明するための概略ブロック図である。

【0102】携帯電話機100は、携帯電話網により無線伝送される信号を受信するためのアンテナ1102と、アンテナ1102からの信号を受けてベースバンド

信号に変換し、あるいは携帯電話機からのデータを変調してアンテナ1102に与えるための送受信部1104と、携帯電話機100の各部のデータ授受を行なうためのバスBS2と、バスBS2を介して携帯電話機100の動作を制御するためのコントローラ1106とを含む。

【0103】携帯電話機100は、さらに、外部からの指示を携帯電話機100に与えるためのキー操作部1108と、コントローラ1106等から出力される情報を携帯電話ユーザに視覚情報として与えるためのディスプレイ1110と、通常の通話動作において、データベースBS2を介して与えられる受信データに基づいて音声を再生するための音声再生部1112とを含む。

【0104】携帯電話機100は、さらに、音声再生部1112の出力をディジタル信号からアナログ信号に変換するDA変換器1113と、DA変換器1113の出力を外部出力装置等へ出力するための端子1114とを含む。

【0105】携帯電話機100は、さらに、通常の通話動作において、携帯電話機100のユーザが話した音声信号を入力するマイク1115と、マイク1115からの音声信号をアナログ信号からディジタル信号に変換するAD変換器1116と、AD変換器1116からのディジタル信号を所定の方式に従って符号化してバスBS2へ与える音声符号化部1117とを含む。

【0106】携帯電話機100は、さらに、配信サーバ30からのコンテンツデータ（音楽データ）を記憶しつつ復号化処理するための着脱可能なメモリカード110と、メモリカード110とバスBS2との間のデータの授受を制御するためのメモリインタフェース1200とを含む。

【0107】携帯電話機100は、さらに、携帯電話機の種類（クラス）ごとにそれぞれ設定される、公開暗号鍵KPp1およびクラス証明書Crtf1を公開復号鍵KPmaで復号することでの正当性を認証できる状態に暗号化した認証データ[KPp1//Crtf1]KPmaを保持する認証データ保持部1202を含む。ここで、携帯電話機（データ端末装置）100のクラスは、n=1であるとする。

【0108】携帯電話機100は、さらに、携帯電話機（コンテンツ再生回路）固有の復号鍵で暗号化されたKp1保持部1204と、バスBS2から受けたデータをKp1によって復号しメモリカード110によって発生されたセッションキーKs2を得る復号処理部1206とを含む。

【0109】携帯電話機100は、さらに、メモリカード110に記憶されたコンテンツデータの再生を行なう再生セッションにおいてメモリカード110の間でバスBS2上においてやり取りされるデータを暗号化するためのセッションキーKs3を乱数等により発生するセ

セッションキー発生部1210と、発生されたセッションキーKs3を復号処理部1206によって得られたセッションキーKs2によって暗号化しバスBS2に出力する暗号化処理部1208とを含む。

【0110】携帯電話機100は、さらに、バスBS2上のデータをセッションキーKs3によって復号して出力する復号処理部1212とを含む。

【0111】携帯電話機100は、さらに、バスBS2より暗号化コンテンツデータ{Data}Kcを受けて、復号処理部1212より取得したライセンス鍵Kcによって復号しコンテンツデータを出力する復号処理部1214と、復号処理部1214の出力を受けてコンテンツデータを再生するための音楽再生部1216と、音楽再生部1216の出力をデジタル信号からアナログ信号に変換するDA変換器1218と、DA変換器1218とDA変換器1218との出力を受けて、動作モードに応じて選択的に端子1114または端子1220から出力するためのスイッチ1222と、スイッチ1222の出力を受けて、ヘッドホン130と接続するための接続端子1224とを含む。

【0112】なお、図6においては、説明の簡素化のため、携帯電話機のうち本発明の音楽データの配信および再生にかかわるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、一部記載を省略している。

【0113】携帯電話機100の各構成部分の各セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【0114】図7は、メモリカード110の構成を説明するための概略ブロック図である。既に説明したように、メモリカードに固有の公開暗号鍵および秘密復号鍵として、KpmeiおよびKmeiが設けられ、メモリカードのクラス証明書Cmeiが設けられるが、メモリカード110においては、これらは自然数i=1でそれぞれ表わされるものとする。

【0115】したがって、メモリカード110は、認証データ[Kpmei/Kmei]Kpmaを保持する認証データ保持部1400と、メモリカードの種類ごとに設定される固有の復号鍵であるKmc1を保持するKmc1保持部1402と、メモリカードごとに固有に設定される秘密復号鍵Km1を保持するKm1保持部1421と、Km1によって復号可能な公開暗号鍵Kpm1を保持するKpm1保持部1416とを含む。認証データ保持部1400は、メモリカードの種類およびクラスごとにそれぞれ設定される秘密暗号鍵Kpmeiおよびクラス証明書Cmeiを公開認証鍵Kpmaで復号することでその正当性を確認できる状態に暗号化した認証データ[Kpmei/Kmei]Kpmaとして保持する。

【0116】このように、メモリカードという記録装置

の暗号鍵を設けることによって、以下の説明で明らかになるように、配信されたコンテンツデータや暗号化されたライセンス鍵の管理をメモリカード単位で実行することが可能になる。

【0117】メモリカード110は、さらに、メモリインタフェース1200との間で信号を端子1201を介して授受するインタフェース1423と、インタフェース1423との間で信号をやり取りするバスBS3と、バスBS3にインタフェース1423から与えられるデータから、メモリカードの種類ごとに固有の秘密復号鍵Kmc1をKmc1保持部1402から受けて、配信サーバ30が配信セッションにおいて生成したセッションキーKs1を接点Paに出力する復号処理部1404

と、Kpma保持部1414から認証鍵Kpmaを受けて、バスBS3に与えられるデータからKpmaによる復号処理を実行して復号結果を暗号化処理部1410に出力する復号処理部1408と、切換えスイッチ1442によって選択的に与えられる鍵によって、切換えスイッチ1444によって選択的に与えられるデータを暗号化してバスBS3に出力する暗号化処理部1406とを含む。

【0118】メモリカード110は、さらに、配信、および再生の各セッションにおいてセッションキーKs2を発生するセッションキー発生部1418と、セッションキー発生部1418の出力したセッションキーKs2を復号処理部1408によって得られる公開暗号鍵KpniもしくはKpmeiによって暗号化してバスBS3に送出する暗号化処理部1410と、バスBS3よりセッションキーKs2によって暗号化されたデータを受けてセッションキー発生部1418より得たセッションキーKs2によって復号し、復号結果をバスBS4に送出する復号処理部1412とを含む。

【0119】メモリカード110は、さらに、バスBS3上のデータを公開暗号鍵Kpm1と対をなすメモリカード110固有の秘密復号鍵Km1によって復号するための復号処理部1422と、禁止クラスリストのバージョン更新のためのデータCRL\_dataによって逐次更新される禁止クラスリストデータCRLをバスB4より受けて格納するとともに、暗号化コンテンツデータ

{Data}Kcおよび付加情報Data-infをバスBS3より受けて格納するためのメモリ1415とを含む。メモリ1415は、例えば半導体メモリによって構成される。また、メモリ1515は、禁止クラスリストCRLを記録したCRL領域1415Aと、コンテンツIDを含むHeader、暗号化コンテンツデータ{Data}Kc、および暗号化コンテンツデータの関連情報Data-infを記録したデータ領域1415Bとから成る。

【0120】メモリカード110は、さらに、復号処理部1422によって得られるライセンスを保持するため

のライセンス情報保持部1440と、バスBS3を介して外部との間でデータ授受を行ない、バスBS4との間で再生情報等を受けて、メモリカード110の動作を制御するためのコントローラ1420を含む。

【0121】ライセンス情報保持部1440は、N個(N:自然数)のバンクを有し、各ライセンスに対応するライセンスをバンクごとに保持する。

【0122】なお、図7において、実線で囲んだ領域は、メモリカード110内において、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読出を不能化するためのモジュールTRMに組込まれているものとする。このようなモジュールは、一般にはタンパーレジスタンスモジュール(Tamper Resistance Module)である。

【0123】もちろん、メモリ1415も含めて、モジュールTRM内に組込まれる構成としてもよい。しかしながら、図7に示したような構成とすることで、メモリ1415中に保持されている再生に必要な再生情報は、いずれも暗号化されているデータであるため、第三者はこのメモリ1415中のデータのみでは、音楽を再生することは不可能であり、かつ高価なタンパーレジスタンスモジュール内にメモリ1415を設ける必要がないので、製造コストが低減されるという利点がある。

【0124】以降では、簡単化のためアクセス制御情報AC1は再生回数の制限を行なう制御情報である再生回数のみを、再生回路制御情報AC2は再生可能な期限を規定する制御情報である再生期限のみを制限するものとし、アクセス制御情報AC1および再生回路制御情報AC2を、それぞれ、再生回数制限AC1、再生期限AC2と称するものとする。

【0125】図8を参照して、暗号化コンテンツデータ[Data]Kcと、ライセンス鍵Kc、再生回数制限AC1、および再生期限AC2等から成るライセンスとが記録されたメモリカード110における各種の状態について説明する。なお、図8においては、再生回数制限AC1に制限がない場合を「FF」で表し、再生期限AC2に制限がない場合を「00」で表している。図8の(a)は、暗号化コンテンツデータ[Data]Kcおよびライセンスがメモリカード110に記録されており、新たに暗号化コンテンツデータ[Data]Kcとライセンスとを配信サーバ30から受信する場合を示す。また、図8の(b)は、暗号化コンテンツデータ[Data]Kcおよびライセンス鍵Kcが存在し、一部、再生回数制限AC1によって暗号化コンテンツデータ[Data]Kcの再生が制限されている場合を示す。さらに、図8の(c)は、暗号化コンテンツデータ[Data]Kcとライセンスとが記録されており、一部の暗号化コンテンツデータ[Data]Kcを再生す

るライセンスが記録されていない場合を示す。

【0126】図8の(a)を参照して、コンテンツID:55019930112、55019951013、55019630122によって特定される暗号化コンテンツデータ:[Data(55019930112)]Kc(55019930112)、[Data(55019951013)]Kc(55019951013)、[Data(55019630122)]Kc(55019630122)、その暗号化コンテンツデータを復号するためのライセンス鍵:AAF53951046FD356ABCC、96F539510456AB332C55、96F5395104AF3323C31が記録されている。また、コンテンツID:55019951013、55019630122によって特定される暗号化コンテンツデータは再生回数制限AC1および再生期限AC2が無制限であるが、コンテンツID:55019930112によって特定される暗号化コンテンツデータの再生回数制限AC1は20回、再生期限AC2は無制限である。したがって、データ領域1415Bに記録された3つの暗号化コンテンツデータ[Data]Kcに対するライセンスはライセンス情報保持部1440に記録されている。

【0127】図8の(b)を参照して、コンテンツID:55019930112、55019951013によって特定される暗号化コンテンツデータ:[Data(55019930112)]Kc(55019930112)、[Data(55019951013)]Kc(55019951013)、その暗号化コンテンツデータを復号するためのライセンス鍵:AAF53951046FD356ABCC、96F539510456AB332C55が記録されている。また、コンテンツID:55019951013によって特定される暗号化コンテンツデータは再生回数制限AC1および再生期限AC2が無制限であるが、コンテンツID:55019930112によって特定される暗号化コンテンツデータの再生回数制限AC1は0回、再生期限AC2は無制限である。したがって、データ領域1415Bに記録された2つの暗号化コンテンツデータ[Data]Kcのうち、1つの暗号化コンテンツデータはライセンスがライセンス情報保持部1440に記録されていない。

【0128】図8の(c)を参照して、コンテンツID:55019930112、55019951013によって特定される暗号化コンテンツデータ:[Data(55019930112)]Kc(55019930112)、[Data(55019951013)]Kc(55019951013)、その暗号化コンテンツデータを復号するためのライセンス鍵:AAF53951046FD356ABCC、96F539510456AB332C55が記録されている。また、コンテ

ンツID:55019951013によって特定される暗号化コンテンツデータは再生回数制限AC1および再生期限AC2が無制限であり、コンテンツID:55019930112によって特定される暗号化コンテンツデータの再生回数制限AC1は20回、再生期限AC2は無制限である。さらに、コンテンツID:55019630122によって特定される暗号化コンテンツデータ: [Data (55019630122)] Kc (55019630122) はデータ領域1415Bに記録されているが、その暗号化コンテンツデータを再生するためのライセンス鍵Kc、再生回数制限AC1、および再生期限AC2から成るライセンスはライセンス情報保持部1440に記録されていない。したがって、データ領域1415Bに記録された3つの暗号化コンテンツデータ [Data] Kcのうち、1つの暗号化コンテンツデータに対するライセンスが存在しない。

【0129】図8を参照して説明するように、メモ리카ード110には、暗号化コンテンツデータ [Data] Kc、ライセンス鍵Kc、再生回数制限AC1、および再生期限AC2が記録されているか否かによって各種の状態が存在する。

【0130】次に、暗号化コンテンツデータ [Data] Kc、およびライセンス鍵Kc等が各種の状態で記録されたメモ리카ード110が携帯電話機100に装着され、携帯電話機100のユーザから暗号化コンテンツデータの受信要求がされた場合の動作について説明する。

【0131】図9～図12は、図1に示すデータ配信システムにおける暗号化コンテンツデータの購入時に発生する配信動作（以下、配信セッションともいう）を説明するための第1～第4のフローチャートである。

【0132】図9を参照して、携帯電話機100のユーザからキー操作部1108を介してコンテンツデータの配信要求がなされると、携帯電話機100は、コンテンツメニューの送信要求を配信サーバ30へ送信する（ステップS70）。配信サーバ30の配信制御部315は、通信装置350およびバスBS1を介してコンテンツメニューの送信要求を受信すると（ステップS72）、メニューデータベース307からバスBS1を介してコンテンツメニューを読み出し、その読み出したコンテンツメニューをバスBS1および通信装置350を介して携帯電話機100へ送信する（ステップS74）。携帯電話機110は、送受信部1104によってコンテンツメニューを受信し、コントローラ1106は、コンテンツメニューを表示部1110に表示する（ステップS76）。

【0133】そうすると、携帯電話機100の表示部1110には、図13に示すコンテンツメニュー60が表示される。ユーザは、コンテンツメニュー60の番号001、002、003、・・・を選択することによって

配信を希望する暗号化コンテンツデータを選択する。表示部1110には、別の画面に移行するための移行部1111が設けられている。ユーザは、表示部1110に表示されたコンテンツメニュー60中に希望する暗号化コンテンツデータが表示されていないとき、移行部1111をクリックする。移行部1111には、別の画面へ移行するためのアドレスが含まれている。

【0134】携帯電話機100のコントローラ1106は、コンテンツが選択された否かを判断し（ステップS78）、移行部1111がクリックされると、コントローラ1106は、移行部1111に含まれるアドレスを送受信部1104を介して配信サーバ30へ送信し、別の画面を送信するように要求する。そして、ステップS70～S78が繰返される。つまり、コンテンツメニューは、コンテンツメニュー60から成る複数個の画面が階層的に配列されて構成されており、各画面は、ジャンルの異なる暗号化コンテンツデータ、同じジャンルであるが、他の暗号化コンテンツデータ等から成るコンテンツメニューによって構成されている。

【0135】そして、配信サーバ30から複数の画面によって送られてきたコンテンツメニューに、希望する暗号化コンテンツデータが含まれていないとき、配信動作はステップS170へ移行し、配信動作は終了する。

【0136】コンテンツメニュー60は、暗号化コンテンツデータを特定するためのコンテンツIDを含んでおり、ステップS78において暗号化コンテンツデータが選択されたとき、コンテンツメニューから選択された暗号化コンテンツデータのコンテンツIDが抽出される（ステップS80）。

【0137】そして、キー操作部1108を介して暗号化コンテンツデータのライセンスを購入するための購入条件ACが入力される（ステップS82）。つまり、選択した暗号化コンテンツデータを復号するライセンス鍵Kcを購入するために、暗号化コンテンツデータの再生回数制限AC1、および再生期限AC2を設定して購入条件ACが入力される。

【0138】暗号化コンテンツデータの購入条件ACが入力されると、コントローラ1106は、選択された暗号化コンテンツデータに対するコンテンツIDと同じコンテンツIDを有する暗号化コンテンツデータ [Data] Kcがメモ리카ード110に記録されていないかを検索する（ステップS84）。この場合、コントローラ1106は、選択された暗号化コンテンツデータに対応するコンテンツIDをメモリアインタフェース1200を介してメモ리카ード110へ送信する。メモ리카ード110のコントローラ1420は、インタフェース1423およびバスBS3を介して携帯電話機100からコンテンツIDを受取り、その受取ったコンテンツIDがメモリア1415のHeader 1424に含まれるコンテンツIDと一致するか否かによって、ユーザがコンテ

ツメニューから選択した暗号化コンテンツデータがメモリーカード110に記録されているか否かを検索する。

【0139】この場合、メモリーカード110のメモリ415に記録されたHeader、Data-inf、および【Data】Kcを図14に示すように1つのデータ列としてハッシュ関数などを用いた署名データを併せて取扱うようにすれば、コンテンツIDの改組を防止することができる。署名の確認は、コンテンツIDの検査時に対応したものに限りても行なえば良い。

【0140】そして、コントローラ1106は、選択した暗号化コンテンツデータがメモリーカード110に記録されているか否かを判断し（ステップS86）、暗号化コンテンツデータがメモリーカード110に記録されていないとき、データを配信サーバ30から取得するためのフラグ“Yes”を立てる（ステップS88）。暗号化コンテンツデータがメモリーカード110に記録されているとき、ライセンスの確認が行なわれる（ステップS90）。つまり、図8を参照して説明したようにライセンス鍵Kcがメモリーカード110に記録されているか、再生回数制限AC1および再生期限AC2によって暗号化コンテンツデータの再生が制限されないかによってライセンスの確認が行なわれる。ライセンスが存在しないときはステップS94へ移行する。ライセンスが存在し、暗号化コンテンツデータが再生できる場合、コントローラ1106は、「ライセンス単体購入？」を表示部1110に表示し、ライセンスだけを単体で購入するか否かの意思を確認する（ステップS92）。コントローラ1106は、ライセンスだけを購入しない旨の指示がキー操作部1108から入力されると、ステップS170へ移行し、暗号化コンテンツデータの配信動作は終了する。コントローラ1106は、ライセンスだけを単体で購入する旨の指示がキー操作部1108から入力されると、データを配信サーバ30から取得しないフラグ“No”を立てる（ステップS94）。

【0141】次に、図10を参照して、携帯電話機100は、ユーザが暗号化コンテンツデータを選択することによって抽出したコンテンツID（ステップS80参照）の指定による配信リクエストがなされる（ステップS100）。

【0142】メモリーカード110においては、この配信リクエストに応じて、認証データ保持部1400より認証データ【KPMC1／／Cmc1】KPmaが出力される（ステップS102）。

【0143】携帯電話機100は、メモリーカード110からの認証のための認証データ【KPMC1／／Cmc1】KPmaに加えて、コンテンツID、ライセンス購入条件のデータACと配信サーバ30に対して送信する（ステップS104）。

【0144】配信サーバ30では、携帯電話機100からコンテンツID、認証データ【KPMC1／／Cmc

1】KPma、ライセンス購入条件のデータACを受信し（ステップS106）、復号処理部312においてメモリーカード110から出力された認証データを公開認証鍵KPmaで復号処理を実行する（ステップS108）。

【0145】配信制御部315は、復号処理部312における復号処理結果から、処理が正常に行なわれたか否か、すなわち、メモリーカード110が正規のメモリーカードからの公開暗号鍵KPmc1と証明書Cmc1を保持することを認証するために、正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう（ステップS110）。正当な認証データであると判断された場合、配信制御部315は、公開暗号鍵KPmc1および証明書Cmc1を承認し、受理する。そして、次の処理（ステップS112）へ移行する。正当な認証データでない場合には、非承認とし、公開暗号鍵KPmc1および証明書Cmc1を受理しないで処理を終了する（ステップS170）。

【0146】認証の結果、正規の機器であることが認識されると、配信制御部315は、次に、メモリーカード110のクラス証明書Cmc1が禁止クラスリストCRLにリストアップされているかどうかをCRLデータベース306に照会し、これらのクラス証明書が禁止クラスリストの対象になっている場合には、ここで配信セッションを終了する（ステップS170）。

【0147】一方、メモリーカード110のクラス証明書が禁止クラスリストの対象外である場合には次の処理に移行する（ステップS112）。

【0148】認証の結果、正当な認証データを持つメモリーカードを備える携帯電話機からのアクセスであり、クラスが禁止クラスリストの対象外であることが確認されると、配信サーバ30において、配信制御部315は、配信を特定するための管理コードであるトランザクションIDを生成する（ステップS113）。また、セッションキー発生部316は、配信のためのセッションキーKs1を生成する。セッションキーKs1は、復号処理部312によって得られたメモリーカード110に対応する公開暗号鍵KPmc1によって、暗号化処理部318によって暗号化される（ステップS114）。

【0149】トランザクションIDおよび暗号化されたセッションキーKs1は、トランザクションID／／【Ks1】Kmc1として、バスB3および通信装置350を介して外部に出力される（ステップS116）。

【0150】携帯電話機100が、トランザクションID／／【Ks1】Kmc1を受信すると（ステップS118）、メモリーカード110においては、メモリーインタフェース1200を介して、バスB3に与えられた受信データを、復号処理部1404が、保持部1402に

保持されるメモリカード110固有の秘密復号鍵Kmc1により復号処理することにより、セッションキーKs1を復号し抽出する(ステップS120)。

【0151】コントローラ1420は、配信サーバ30で生成されたセッションキーKs1の受理を確認すると、セッションキー発生部1418に対して、メモリカード110において配信動作時に生成されるセッションキーKs2の生成を指示する。

【0152】また、配信セッションにおいては、コントローラ1420は、メモリカード110内のメモリ1415に記録されている禁止クラシストのデータCRL\_datをメモリ1415から抽出してバスBS4に出力する。

【0153】暗号化処理部1406は、切換スイッチ1442の接点Paを介して復号処理部1404より与えられるセッションキーKs1によって、切換スイッチ1444および1446の接点を順次切換えることによって与えられるセッションキーKs2、公開暗号鍵Kpm1および禁止クラシストのデータCRL\_datを1つのデータ列として暗号化して、[Ks2//Kpm1//CRL\_dat] Ks1をバスBS3に出力する(ステップS122)。

【0154】バスBS3に出力された暗号化データ[Ks2//Kpm1//CRL\_ver] Ks1は、バスBS3からインタフェース1423、端子1201およびメモリインタフェース1200を通じて携帯電話機100に出力され、携帯電話機100から配信サーバ30に送信される(ステップS124)。

【0155】配信サーバ30は、トラザクションID//[Ks2//Kpm1//CRL\_dat] Ks1を受信して、復号処理部320においてセッションキーKs1による復号処理を実行し、メモリカード110で生成されたセッションキーKs2、メモリカード110固有の公開暗号鍵Kpm1およびメモリカード110における禁止クラシストのデータCRL\_datを受理する(ステップS126)。

【0156】配信制御部315は、ステップS106で取得したコンテンツIDおよびライセンス購入条件のデータACに従って、ライセンスID、アクセス制限情報AC1および再生期限AC2を生成する(ステップS128)。さらに、暗号化コンテンツデータを復号するためのライセンス鍵Kcを情報データベース304より取得する(ステップS130)。

【0157】配信制御部315は、生成したライセンス、すなわち、ライセンス鍵Kc、再生期限AC2、ライセンスID、コンテンツID、およびアクセス制限情報AC1を暗号化処理部326に与える。暗号化処理部326は、復号処理部320によって得られたメモリカード110固有の公開暗号鍵Kpm1によってライセンスを暗号化する(ステップS132) 図11を参照し

て、配信サーバ30において、メモリカード110から送信された禁止クラシストのデータCRL\_datが最新か否かが判断され、データCRL\_datが最新と判断されたとき、ステップS134へ移行する。また、データCRL\_datが最新でないときはステップS137へ移行する(ステップS133)。

【0158】データCRL\_datが最新と判断されたとき、暗号化処理部328は、暗号化処理部326から出力された暗号化データ[Kc//AC2//ライセンスID//コンテンツID//AC1] Km1をメモリカード110において発生されたセッションキーKs2によって暗号化を行い、暗号化データ[Kc//AC2//ライセンスID//コンテンツID//AC1] Km1 Ks2をバスBS1に出力する。そして、配信制御部315は、バスBS1上の暗号化データ[Kc//AC2//ライセンスID//コンテンツID//AC1] Km1 Ks2を通信装置350を介して携帯電話機100へ送信する(ステップS134)。

【0159】そして、携帯電話機100は、暗号化データ[Kc//AC2//ライセンスID//コンテンツID//AC1] Km1 Ks2を受信し(ステップS135)、バスBS2およびメモリインタフェース1200を介してメモリカード110へ送信する。メモリカード110の復号処理部1412は、暗号化データ[Kc//AC2//ライセンスID//コンテンツID//AC1] Km1 Ks2を端子1201およびインタフェース1423を介して受取り、セッションキー発生部1418によって発生されたセッションキーKs2によって復号し、[Kc//AC2//ライセンスID//コンテンツID//AC1] Km1を受理する(ステップS136)。その後、ステップS146へ移行する。

【0160】一方、配信サーバ30において、CRL\_datが最新でないと判断されると、配信制御部315は、バスBS1を介してCRLデータベース306から最新の禁止クラシストのデータCRL\_datを取得する(ステップS137)。

【0161】暗号化処理部328は、暗号化処理部326の出力と、配信制御部315がバスBS1を介して供給する禁止クラシストの最新データCRL\_datとを受けて、メモリカード110において生成されたセッションキーKs2によって暗号化する。暗号化処理部328より出力された暗号化データは、バスBS1および通信装置350を介して携帯電話機100に送信される(ステップS138)。

【0162】このように、配信サーバおよびメモリカードでそれぞれ生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行な



うことができ、データ配信システムのセキュリティを向上させることができる。

【0163】携帯電話機100は、送信された暗号化データ [Kc//AC2//ライセンスID//コンテンツID//AC1] Km1//CRL\_dat] Ks2を受信し(ステップS140)、メモリインタフェース1200を介してメモリカード110へ出力する。メモリカード110においては、端子1201およびインタフェース1423を介して、バスBS3に与えられた受信データを復号処理部1412によって復号する。復号処理部1412は、セッションキー発生部1418から与えられたセッションキーKs2を用いてバスBS3の受信データを復号しバスBS4に出力する(ステップS142)。

【0164】この段階で、バスBS4には、Km1保持部1421に保持される秘密復号鍵Km1で復号可能な暗号化ライセンス [Kc//AC2//ライセンスID//コンテンツID//AC1] Km1と、CRL\_datとが出力される(ステップS142)。コントローラ1420の指示によって受理した最新の禁止クラスリストCRL\_datによってメモリ1415内の禁止クラスリストCRLが書き換えられる(ステップS144)。

【0165】ステップS134、S135、S136は、メモリカード110から送られてきた禁止クラスリストCRL\_datが最新のもののライセンス鍵Kc等のメモリカード110への配信動作であり、ステップS137、S138、S140、S142、S144は、メモリカード110から送られてきた禁止クラスリストCRL\_datが最新でないもののライセンス鍵Kc等のメモリカード110への配信動作である。このように、メモリカード110から送られてきた禁止クラスリストCRL\_datが更新されているかを、逐一、確認し、更新されないとき、最新の禁止クラスリストCRL\_datをCRLデータベース306から取得し、メモリカード110に配信することによって、ライセンスの破れたメモリカードへの暗号化コンテンツデータ [Data] Kcの配信を防止し、かつ、ライセンスの破れた携帯電話機による暗号化コンテンツデータ [Data] Kcの再生を防止できる。

【0166】ステップS136またはステップS144の後、コントローラ1420の指示によって、暗号化ライセンス [Kc//AC2//ライセンスID//コンテンツID//AC1] Km1は、復号処理部1422において、秘密復号鍵Km1によって復号され、ライセンス(ライセンス鍵Kc)、ライセンスID、コンテンツID、再生回数制限AC1および再生期限AC2が受理される(ステップS148)。

【0167】コントローラ1420は、ライセンスをライセンス情報保持部1440に記録する(ステップS1

50)。

【0168】図12を参照して、携帯電話機100のコントローラ1106は、ステップS88およびステップS94において立てたフラグを参照し、配信サーバ30から暗号化コンテンツデータを取得するか否かを判断する。そして、暗号化コンテンツデータを配信サーバ30から取得しないと、ステップS164へ移行し、暗号化コンテンツデータを配信サーバ30から取得すると、ステップS154へ移行する。

【0169】暗号化コンテンツデータを配信サーバ30から取得するとき、携帯電話機100は、配信サーバ30から送られたトランザクションIDと、暗号化コンテンツデータの配信要求を配信サーバ30へ送信する(ステップS154)。

【0170】配信サーバ30は、トランザクションIDおよび暗号化コンテンツデータの配信要求を受信し(ステップS156)、情報データベース304より、暗号化コンテンツデータ [Data] Kcおよび付加情報Data\_infを取得して、これらのデータをバスBS1および通信装置350を介して出力する(ステップS158)。

【0171】携帯電話機100は、[Data] Kc//Data\_infを受信して、暗号化コンテンツデータ [Data] Kcおよび付加情報Data\_infを受理する(ステップS160)。暗号化コンテンツデータ [Data] Kcおよび付加情報Data\_infは、メモリインタフェース1200、端子1201、およびインタフェース1423を介してメモリカード110のバスBS3に伝達される。メモリカード110においては、受信した暗号化コンテンツデータ [Data] Kcおよび付加情報Data\_infがそのままメモリ1415に記録される(ステップS162)。

【0172】そして、ステップS152において暗号化コンテンツデータを配信サーバ30から受信しないと判断されたときも含め、メモリカード110から配信サーバ30へは、トランザクションID//配信受理の通知が送信され(ステップS164)、配信サーバ30でトランザクションID//配信受理を受信すると(ステップS166)、課金データベース302への課金データの格納、およびトランザクションIDの配信記録データベース308への記録が行われて配信終了の処理が実行され(ステップS168)、全体の処理が終了する(ステップS170)。

【0173】このようにして、携帯電話機100に装着されたメモリカード110が正規の機器であること、同時に、クラス証明書Cmc1とともに暗号化して送信してきた公開暗号鍵Kp1およびKmc1が有効であることを確認した上で、それぞれのクラス証明書Cmc1が禁止クラスリスト、すなわち、公開暗号鍵Kp1およびKmc1による暗号化が破られたクラス証明書リストに記

載されていないメモリカードからの配信要求に対してのみコンテンツデータを配信することができ、不正なメモリカードへの配信および解読されたクラス鍵を用いた配信を禁止することができる。

【0174】また、配信サーバ30への暗号化コンテンツデータ [Data] Kcの配信要求時にメモリカード110における暗号化コンテンツデータ [Data] Kc、ライセンス鍵Kc、および再生回数制限AC1等の記録状況に応じて、必要な配信だけを配信サーバ30に要求することができる。その結果、無駄な配信を防止することができる。

【0175】次に、図15および図16を参照してメモリカード110に配信されたコンテンツデータの携帯電話機100における再生動作について説明する。図15を参照して、再生動作の開始とともに、携帯電話機100のユーザからキー操作部1108を介して再生指示が携帯電話機100にインプットされる(ステップS200)。そうすると、コントローラ1106は、バスBS2を介して認証データ保持部1202から認証データ [Kp1//Crtf1] KPmaを読み出し、メモリインタフェース1200を介してメモリカード110へ認証データ [Kp1//Crtf1] KPmaを入力する(ステップS201)。

【0176】そうすると、メモリカード110は、認証データ [Kp1//Crtf1] KPmaを受理する(ステップS202)。そして、メモリカード110の復号処理部1408は、受理した認証データ [Kp1//Crtf1] KPmaを、KPma保持部1414に保持された公開認証鍵KPmaによって復号し(ステップS203)、コントローラ1420は復号処理部1408における復号処理結果から、認証処理を行なう。すなわち、認証データ [Kp1//Crtf1] KPmaが正規の認証データであるか否かを判断する認証処理を行なう(ステップS204)。復号できなかった場合、コントローラ1420は認証データ不受理の出力をデータBS3および端子1201を介して携帯電話機100のメモリインタフェース1200へ出力する(ステップS206)。認証データが復号できた場合、コントローラ1420は、取得した証明書Crtf1がメモリ1415から読み出した禁止クラスリストデータに含まれるか否かを判断する(ステップS205)。この場合、証明書Crtf1にはIDが付与されており、コントローラ1420は、受理した証明書Crtf1のIDが禁止クラスリストデータの中に存在するか否かを判別する。証明書Crtf1が禁止クラスリストデータに含まれると判断されると、コントローラ1420は認証データ不受理の出力をデータBS3および端子1201を介して携帯電話機100のメモリインタフェース1200へ出力する(ステップS206)。

【0177】ステップS204において認証データが公

開認証鍵KPmaで復号できなかったとき、およびステップS205において受理した証明書Crtf1が禁止クラスリストデータに含まれているとき、認証データ不受理の出力がなされる。そして、携帯電話機100のコントローラ1106は、メモリインタフェース1200を介して認証データ不受理の出力を受けると、認証データ不受理のデータをディスプレイ1110に表示する(ステップS207)。

【0178】ステップS205において、証明書Crtf1が禁止クラスリストデータに含まれていないと判断されると、図16を参照して、メモリカード110のセッションキー発生部1418は、再生セッション用のセッションキーKs2を発生させる(ステップS208)。そして、暗号処理部1410は、セッションキー発生部1418からのセッションキーKs2を、復号処理部1408で復号された公開暗号鍵Kp1によって暗号化した [Ks2] Kp1をバスBS3へ出力する(ステップS209)。そうすると、コントローラ1420は、端子1201を介してメモリインタフェース1200へ [Ks2] Kp1を出力し、携帯電話機100のコントローラ1106は、メモリインタフェース1200を介して [Ks2] Kp1を取得する。そして、Kp1保持部1204は、秘密復号鍵Kp1を復号処理部1206へ出力する。

【0179】復号処理部1206は、Kp1保持部1204から出力された、公開暗号鍵Kp1と対になっている秘密復号鍵Kp1によって [Ks2] Kp1を復号し、セッションキーKs2を暗号処理部1208へ出力する(ステップS210)。そうすると、セッションキー発生部1210は、再生セッション用のセッションキーKs3を発生させ、セッションキーKs3を暗号処理部1208へ出力する(ステップS211)。暗号処理部1208は、セッションキー発生部1210からのセッションキーKs3を復号処理部1206からのセッションキーKs2によって暗号化して [Ks3] Ks2を出力し、コントローラ1106は、バスBS2およびメモリインタフェース1200を介して [Ks3] Ks2をメモリカード110へ出力する(ステップS212)。

【0180】メモリカード110の復号処理部1412は、端子1201、インタフェース1423、およびバスBS3を介して [Ks3] Ks2を入力し、セッションキー発生部1418によって発生されたセッションキーKs2によって [Ks3] Ks2を復号して、携帯電話機100で発生されたセッションキーKs3を取得する(ステップS213)。

【0181】セッションキーKs3の受理に応じて、コントローラ1420は、ライセンス情報保持部1440内の対応するアクセス制限情報AC1を確認する(ステップS214)。

【0182】ステップS214においては、メモリのアクセスに対する制限に関する情報であるアクセス制限情報AC1を確認することにより、既に再生不可の状態である場合には再生動作を終了し、再生回数制限がある場合にはアクセス制限情報AC1のデータを更新し再生可能回数を更新した後に次のステップに進む(ステップS215)。一方、アクセス制限情報AC1によって再生回数制限が制限されていない場合においては、ステップS215はスキップされ、再生回数制限AC1は更新されることなく処理が次のステップ(ステップS216)に進行される。

【0183】また、ライセンス情報保持部1440内にリクエスト曲の当該コンテンツIDが存在しない場合においても、再生不可の状態であると判断して、再生動作を終了する。

【0184】ステップS214において、当該再生動作において再生が可能であると判断された場合には、ライセンス情報保持部1440に記録された再生リクエスト曲のライセンス鍵Kcおよび再生期限AC2がバスBS4に出力される(ステップS216)。

【0185】得られたライセンス鍵Kcと再生期限AC2は、切換スイッチ1444の接点Pdを介して暗号化処理部1406に送られる。暗号化処理部1406は、切換スイッチ1442の接点Pdを介して復号処理部1412より受けたセッションキーKs3によってバスB4から受けたライセンス鍵Kcと再生期限AC2とを暗号化し、[Kc//AC2]Ks3をバスBS3に出力する(ステップS217)。

【0186】バスBS3に出力された暗号化データは、インタフェース1423、端子1202、およびメモリインタフェース1200を介して携帯電話機100に送出される。

【0187】携帯電話機100においては、メモリインタフェース1200を介してバスBS2に伝達される暗号化データ[Kc//AC2]Ks3を復号処理部1212によって復号処理を行ない、ライセンス鍵Kcおよび再生期限AC2を受理する(ステップS218)。復号処理部1212は、ライセンス鍵Kcを復号処理部1214に伝達し、再生期限AC2をバスBS2に出力する。

【0188】コントローラ1106は、バスBS2を介して、再生期限AC2を受理して再生の可否の確認を行う(ステップS219)。

【0189】ステップS219においては、再生期限AC2によって再生不可と判断される場合には、再生動作は終了される。

【0190】ステップS219において再生可能と判断された場合、コントローラ1106は、メモリインタフェース1200を介してメモリカード110に暗号化コンテンツデータ[Data]Kcを要求する。そうす

と、メモリカード110のコントローラ1420は、メモリ1415から暗号化コンテンツデータ[Data]Kcを取得し、バスBS3および端子1201を介してメモリインタフェース1200へ出力する(ステップS220)。

【0191】携帯電話機100のコントローラ1106は、メモリインタフェース1200を介して暗号化コンテンツデータ[Data]Kcを取得し、バスBS2を介して暗号化コンテンツデータ[Data]Kcを復号処理部1214へ与える。そして、復号処理部1214は、暗号化コンテンツデータ[Data]Kcを復号処理部1212から出力されたコンテンツ鍵Kcによって復号してコンテンツデータDataを取得する(ステップS221)。

【0192】そして、復号されたコンテンツデータDataは音楽再生部1216へ出力され、音楽再生部1216は、コンテンツデータを再生し、DA変換器1218はデジタル信号をアナログ信号に変換して端子1220へ出力する。そして、スイッチ1222は端子1220を選択して音楽データは端子1224を介してヘッドホン130へ出力されて再生される(ステップS222)。これによって再生動作が終了する。

【0193】図17を参照して、メモリカード110における暗号化コンテンツデータ[Data]Kc、およびライセンス鍵Kc等の記録状況に応じた暗号化コンテンツデータ[Data]Kcおよびライセンス鍵Kc等の配信の例について説明する。図17の(a)を参照して、メモリカード110のデータ領域1415Bには、暗号化コンテンツデータ:[Data(55019930112)][Kc(55019951013)][Kc(55019951013)]、[Data(55019630122)][Kc(55019630122)]と、それぞれの関連情報Data-infとが記録されている。また、ライセンス領域1415Aには、コンテンツID:55019930112、トランザクションID:0000000001、ライセンス鍵Kc:AAF53951046FD356ABCC、再生回数制限AC1:00、再生期限AC2:00のライセンスLS1と、コンテンツID:55019951013、トランザクションID:0000000003005、ライセンス鍵Kc:96F539510456AB332C55、再生回数制限AC1:FF、再生期限AC2:00のライセンスLS2とが記録されている。そして、ライセンスLS1については、再生回数制限AC1は「00」であるので、暗号化コンテンツデータ[Data(55019930112)][Kc(55019930112)]を再生できない、すなわち、ライセンスがない状態を示している。また、暗号化コンテンツデータ[Data(55019630122)][Kc(55019630122)]

2)について、コンテンツID、ライセンス鍵Kc、再生回数制限Ac1、および再生期限Ac2が記録されておらず、ライセンスがない状態を示している。つまり、暗号化コンテンツデータ [Data (55019951013)] Kc (55019951013) に対するライセンスLs2だけが存在し、暗号化コンテンツデータ [Data (55019930112)] Kc (55019930112)、および [Data (55019630122)] Kc (55019630122) に対するライセンスが存在しない状況である。

【0194】図17の(a)に示すメモリカード110の状況において、携帯電話機100のユーザからコンテンツID:55019930112によって特定される暗号化コンテンツデータ [Data] Kcの配信要求がキー操作部1108を介して入力されると、図9のステップS70～S78が行なわれ、コンテンツID:55019930112が抽出される(ステップS80)。そして、ステップS82において、「20」回まで再生可能とするライセンスの購入条件ACが入力される。そして、コンテンツID:55019930112によって特定される暗号化コンテンツデータ [Data] Kcがメモリカード110に記録されているかが検索される(ステップS84)。

【0195】この場合、コンテンツID:55019930112によって特定される暗号化コンテンツデータ [Data] Kcは、メモリカード110に暗号化コンテンツデータ [Data (55019930112)] Kc (55019930112) として記録されているので、図9のステップS86を介してステップS90へ移行する。そして、ステップS90において、ライセンスによって暗号化コンテンツデータ [Data (55019930112)] Kc (55019930112) が再生可能か否かが判断される。この場合、再生回数制限Ac1が「00」であるので、暗号化コンテンツデータ [Data (55019930112)] Kc (55019930112) を再生することができない。したがって、ステップS90からステップS94へ移行する。そして、ステップS94においてデータ取得="No"のフラグが立てられた後、ステップS100～ステップS170によって再生回数制限Ac1を「20」回とするライセンスだけが配信サーバ30からメモリカード110に配信される。そして、図17の(b)に示すようにライセンスLs1の再生回数制限Ac1が「20」と変更される。これによって、ライセンスLs1によって暗号化コンテンツデータ [Data (55019930112)] Kc (55019930112) を再生することができる。

【0196】また、図17の(a)に示すメモリカード110の状況において、携帯電話機100のユーザからコンテンツID:55012345678によって特定

される暗号化コンテンツデータ [Data] Kcの配信要求がキー操作部1108を介して入力されると、図9のステップS70～S78が行なわれ、コンテンツID:55012345678が抽出される(ステップS80)。その後、ライセンスの購入条件ACとして、AC1:FF、AC2:00の再生制限なしが入力される(ステップS82)。そして、コンテンツID:55012345678によって特定される暗号化コンテンツデータ [Data] Kcがメモリカード110に記録されているかが検索される(ステップS84)。この場合、コンテンツID:55012345678によって特定される暗号化コンテンツデータ [Data] Kcはメモリカード110に記録されていないので、ステップS86からステップS88へ移行し、ステップS88においてデータ取得="Yes"のフラグが立てられる。

【0197】その後、ステップS100～ステップS170が実行され、メモリカード110にコンテンツID:55012345678、トランザクションID:00005500345、ライセンス鍵Kc:C6F569510456AB333C4、再生回数制限Ac1:FF、再生期限Ac2:00、暗号化コンテンツデータ: [Data (55012345678)] Kc (55012345678)、および関連情報Data D-inf (55012345678) が配信され、かつ、記録される。これによって、メモリカード110は、図17の(c)に示す状態になり、ユーザが配信要求を行なった暗号化コンテンツデータ [Data (55012345678)] Kc (55012345678) の再生が可能となる。

【0198】さらに、図17の(a)に示すメモリカード110の状況において、携帯電話機100のユーザからコンテンツID:55019630122によって特定される暗号化コンテンツデータ [Data] Kcの配信要求がキー操作部1108を介して入力されると、図9のステップS70～S78が行なわれ、コンテンツID:55019630122が抽出される(ステップS80)。その後、ライセンスの購入条件ACとして、AC1:FF、AC2:00の再生制限なしが入力される(ステップS82)。そして、コンテンツID:55019630122によって特定される暗号化コンテンツデータ [Data] Kcがメモリカード110に記録されているかが検索される(ステップS84)。この場合、コンテンツID:55019630122によって特定される暗号化コンテンツデータ [Data] Kcはメモリカード110に記録されているので、ステップS86からステップS90へ移行する。そして、ステップS90において、ライセンスによって暗号化コンテンツデータ [Data (55019630122)] Kc (55019630122) が再生可能か否かが判断さ

れる。この場合、コンテンツID、ライセンス鍵Kc、再生回数制限AC1、および再生期限ACのいずれもメモ리카ード110に記録されていないので、暗号化コンテンツデータ [Data (55019630122)] Kc (55019630122) を再生することができない。したがって、ステップS90からステップS94へ移行する。

【0199】そして、ステップS94においてデータ取得="No"のフラグが立てられた後、ステップS100～ステップS170によって再生制限なしとするライセンスだけが配信サーバ30からメモ리카ード110に配信される。そして、図17の(d)に示すようにコンテンツID: 55019630122、トランザクションID: 000000550339、ライセンス鍵Kc: F6F53695104AF3323C31、再生回数制限AC1: FF、および再生期限: 00がメモ리카ード110のライセンス領域1415Aに記録される。これによって、暗号化コンテンツデータ [Data (55019630122)] Kc (55019630122) を再生することができる。

【0200】上述したように、携帯電話機100のユーザは、メモ리카ード110における暗号化コンテンツデータ [Data] Kc、およびライセンス鍵Kc等の記録状況に応じて、携帯電話機100を用いて配信サーバ30から暗号化コンテンツデータ [Data] Kcおよびライセンス鍵Kc等をメモ리카ード110に受信し、ライセンス鍵Kcによって暗号化コンテンツデータ [Data] Kcを復号し、かつ、再生することができる。

【0201】上記においては、携帯電話機100のユーザが暗号化コンテンツデータ [Data] Kcの配信要求を行なうとき、メモ리카ード110に記録されている暗号化コンテンツデータ [Data] Kcは、配信サーバ30から受信した暗号化コンテンツデータであるとして説明したが、本発明においては、かかる場合に限らず、配信サーバ30以外から暗号化コンテンツデータ [Data] Kcだけを受信し、メモ리카ード110に記録した場合も含まれる。

【0202】図18および図19を参照して、配信サーバ30以外の装置から暗号化コンテンツデータ [Data] Kcを受信し、その暗号化コンテンツデータ [Data] Kcをメモ리카ード110に記録する場合について説明する。

【0203】図18を参照して、コンピュータ140を用いた暗号化コンテンツデータ [Data] Kcの配信について説明する。携帯電話機100にはメモ리카ード110が着脱可能であり、音楽を再生するためのヘッドホン130が接続されている。そして、携帯電話機100は、通信ケーブル145を介してコンピュータ140と接続されている。

【0204】コンピュータ140は、ハードディスク1

41と、コントローラ142と、外部インタフェース143とを備える。そして、ハードディスク141はバスBS5を介してコントローラ142と接続され、コントローラ142はライセンス保護モジュール143を含む。

【0205】ハードディスク141は、インターネット配信によってコンピュータ140に配信された暗号化コンテンツデータ [Data] KcをバスBS5を介して記憶する。コントローラ142は、携帯電話機100のユーザから通信ケーブル145および外部インタフェース143を介して暗号化コンテンツデータ [Data] Kcの送信要求があると、ハードディスク141から暗号化コンテンツデータ [Data] Kcを読み出し、外部インタフェース143を介して外部へ出力する。

【0206】外部インタフェース143は、携帯電話機100から通信ケーブル145を介してコンピュータ140に入力された信号をコントローラ142に入力するとともに、コントローラ142からの信号を外部へ出力する。

【0207】ライセンス保護モジュール144は、図5に示すデータ処理部310と同じ構成を有し、携帯電話機100に装着されたメモ리카ード110に暗号化コンテンツデータ [Data] Kcを送信するために、上述したように携帯電話機100およびメモ리카ード110と公開暗号鍵、セッションキー等のやり取りを行ないながら、暗号化コンテンツデータ [Data] Kcを保護してメモ리카ード110へ送信するものである。

【0208】インターネット配信によって配信サーバからコンピュータ140に暗号化コンテンツデータ [Data] Kcが配信され、コンピュータ140のハードディスク141にバスBS5を介して暗号化コンテンツデータが記憶されている。

【0209】携帯電話機100のユーザがキー操作部1108から送信要求を入力すると、通信ケーブル145および外部インタフェース143を介して送信要求がコントローラ142に入力される。コントローラ142は、送信要求を受け付けると、要求された暗号化コンテンツデータ [Data] KcをバスBS5を介してハードディスク141から読み出し、ライセンス保護モジュール144に入力する。

【0210】ライセンス保護モジュール144は、上述したようにメモ리카ード110と通信ケーブル145を介して公開暗号鍵、セッションキー等のやり取りを行ない、暗号化コンテンツデータ [Data] Kcをメモ리카ード110へ送信する。

【0211】送信後、携帯電話機100のユーザは、上述したのと同じ方法によって暗号化コンテンツデータ [Data] Kcのライセンス (コンテンツID、ライセンス鍵Kc、再生回数制限AC1、および再生期限AC2) を配信サーバ30から配信してもらい、暗号化コ

ンテンツデータ [Data] Kcを再生する。

【0212】CDを用いた場合、音楽CDから取得して生成した暗号化コンテンツデータ [Data] Kcは、一旦、ハードディスク141に記録してからメモリカード110へ送信しても良いし、ハードディスク141に送信せずに、直接、メモリカード110へ送信しても良い。

【0213】暗号化コンテンツデータ [Data] Kcは、図19に示すようにメモリカード110を、直接、コンピュータ140に装着してメモリカード110に暗号化コンテンツデータ [Data] Kcを記録しても良い。この場合、コンピュータ140のコントローラ142は、ライセンス保護モジュール144によって、直接、メモリカード110に暗号化コンテンツデータを記録する。

【0214】図19においても、コンピュータ140は、図18に示す場合と同じ方法により暗号化コンテンツデータ [Data] Kcを取得する。

【0215】携帯電話機100が、新たに受信した暗号化コンテンツデータ [Data] Kcに対応するライセンス鍵を含むライセンスの配信要求を配信サーバ30へ行なう場合のフローチャート、および新たに受信した暗号化コンテンツデータ [Data] Kcを再生するフローチャートは、図9～図12、および図15、16に示すフローチャートと同じである。

【0216】再生回数期限AC1および再生期限AC2を、それぞれ、再生回数制限と再生期限として説明したが、再生回数期限AC1は記録装置でのライセンスの扱いに制限を加える制御情報であればよく、また、再生回数はデータ再生端末における再生に対して制限を加えるものであれば何れの制限を行ってもかまわない。

【0217】また、携帯電話機100を暗号化コンテンツデータまたはライセンスの配信を受けるデータ端末装置として説明したが、特に通話機能等は必要なく、ただ、暗号化コンテンツデータまたはライセンスの受信を行えるデータ通信機能を備え、受信したデータを記録できればいかなるデータ端末装置であってもよい。

【0218】さらに、携帯電話機100はコンテンツデータ（音楽データ）を再生する機能を備えているが、必ずしもデータ再生機能が必要とせず、ただ、暗号化コンテンツデータまたはライセンスの受信を行えるデータ通信機能を備え、受信したデータを記録できればいかなるデータ端末装置であってもよい。

【0219】またさらに、着脱可能な記録装置であるメモリカードに暗号化コンテンツデータまたはライセンスを記録するように説明したが、メモリカードに限定するものではない。そして、実施の形態においては、着脱可能な記録装置である必要もない。

【0220】本発明の実施の形態によれば、携帯電話機は、ユーザから暗号化コンテンツデータの配信要求が

力されると、装着されたメモリカードの記録状況を検査し、その記録状況に応じて必要な暗号化コンテンツデータ、およびライセンス鍵だけを配信サーバから受信するので、暗号化コンテンツデータ、およびライセンス鍵等が重複してメモリカードに記録されることがない。また、ライセンスを重複して受信することによる無駄な料金を配信サーバへ支払うことを防止できる。さらに、暗号化コンテンツデータを重複して受信することによって無駄な時間が発生するのを防止できる。

【0221】今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【図面の簡単な説明】

【図1】 データ配信システムを概念的に説明する概略図である。

【図2】 図1に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図3】 図1に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図4】 図1に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図5】 ライセンスサーバの構成を示す概略ブロック図である。

【図6】 携帯電話機の構成を示すブロック図である。

【図7】 メモリカードの構成を示すブロック図である。

【図8】 メモリカードの記録状態を説明するための概念図である。

【図9】 図1に示すデータ配信システムにおける配信動作を説明するための第1のフローチャートである。

【図10】 図1に示すデータ配信システムにおける配信動作を説明するための第2のフローチャートである。

【図11】 図1に示すデータ配信システムにおける配信動作を説明するための第3のフローチャートである。

【図12】 図1に示すデータ配信システムにおける配信動作を説明するための第4のフローチャートである。

【図13】 配信サーバから携帯電話機に送信されたコンテンツメニューを携帯電話機の表示部に表示した状態を示す図である。

【図14】 メモリカードのメモリにおけるデータフォーマットである。

【図15】 携帯電話機における再生動作を説明するための第1のフローチャートである。

【図16】 携帯電話機における再生動作を説明するための第2のフローチャートである。

【図17】 メモリカードの記録状況に応じた暗号化コンテンツデータおよびライセンスの配信例を説明する図

である。

【図18】 コンピュータを用いた暗号化コンテンツデータの配信を概念的に説明するための概略図である。

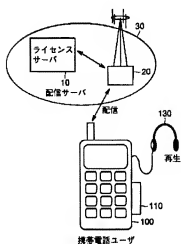
【図19】 コンピュータを用いた暗号化コンテンツデータの配信を概念的に説明するための他の概略図である。

【符号の説明】

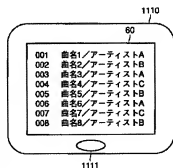
10 ライセンスサーバ、20 配信キャリア、30 配信サーバ、60 コンテンツメニュー、100 携帯電話機、110 メモリカード、130 ヘッドホン、140 コンピュータ、141 ハードディスク、142、1106、1420 コントローラ、143 外部インタフェース、144 ライセンス保護モジュール、145 通信ケーブル、302 課金データベース、304情報データベース、306 CRLデータベース、307 メニューデータベース、308 配信記録データベース、310 データ処理部、312、320、1206、1212、1214、1404、1408、1412、1422復号処理部、313 認証鍵保

持部、315 配信制御部、316、1210、1418 セッションキー発生部、318、326、328、1208、1406、1410 暗号処理部、350 通信装置、1102 アンテナ、1104 送受信部、1108 キー操作部、1110 ディスプレイ、1111 移行部、1112 音声再生部、1113、1218 DA変換器、1114、1201、1220、1224 端子、1115 マイク、1116 AD変換器、1117 音符号号化部、1200 メモリインタフェース、1202、1400 認証データ保持部、1204 Kp1保持部、1216 音楽再生部、1222 スイッチ、1402 Kmc1保持部、1414 KPma保持部、1415 メモリ、1415A CRL領域、1415B データ領域、1416KPm1保持部、1421 Km1保持部、1423 インタフェース、1424 Header、1440 ライセンス情報保持部、1442、1444、1446 切換スイッチ。

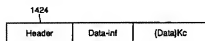
【図1】



【図13】



【図14】



【図4】

名称	属性	保持/発生場所	機能・特徴
Ks1	共通鍵	配信サーバ	配信セッション時に発生
Ks2		メモリカード	配信/再生セッション時に発生
Ks3		携帯電話機	再生セッション時に発生
Km	秘密復号鍵	メモリカード	メモリカードごとに固有の復号鍵 KPmで暗号化されたデータはKmで復号可能
KPm	公開暗号鍵 (非対称鍵)	メモリカード	メモリカードごとに固有の暗号鍵
KPma	公開鍵暗鍵	配信サーバ	配信システム全体で共通。

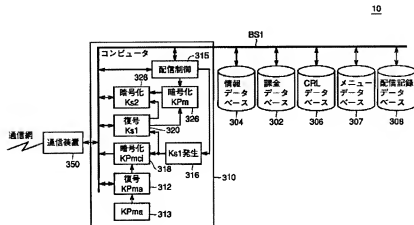
【図2】

名称	属性	保持/発生箇所	機能・特徴
Data	コンテンツデータ	配信サーバ	例：音楽データ、アップデートプログラム
Kc	ライセンス鍵		暗号化コンテンツデータの復号鍵
(Data)Kc	暗号化コンテンツデータ		共通鍵Kcで復号可能な暗号化が施されたコンテンツデータ この形式で配信サーバより配布。
Data-inf	付随情報		例：コンテンツデータに関する著作権あるいはサーバアクセス履歴等の付随情報
コンテンツID	コンテンツに関する情報		コンテンツデータDataを識別するコード
ライセンスID	ライセンスに関する情報		ライセンスの発行を特定できる管理コード (コンテンツIDを含めて識別することも可)
トランザクションID	ライセンス固有		配信を特定するための管理コード
AC	ライセンス購入条件		利用客側から推定(例：ライセンス数、機能限定等)
AC1	アクセス制限情報		メモリのアクセスに対する制限(例：再生可能回数)
AC2	再生回路制御情報		コンテンツ再生回路(読取電話機)における制御情報 (例：再生可否)

【図3】

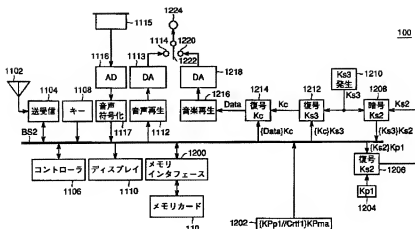
名称	属性	保持/発生箇所	機能・特徴
CRL	配信サーバメモリカード	メモリカード	禁止クラスリストの対象クラスデータ
CRL_dat	禁止クラスリスト関連情報		禁止クラスリストのバージョン更新のための情報
CRL_ver			禁止クラスリストのバージョン情報
KPpn	公開暗号鍵(非対称鍵)	携帯電話機	Kpnにて復号可能。 (KPpn/Crtn)KPmaの形式で出荷時に記録 ※携帯電話機の埋蔵メモリに異なる。
KPmci	公開暗号鍵(非対称鍵)	メモリカード	Kmciにて復号可能。 (KPmci/Cmci)KPmaの形式で出荷時に記録 ※メモリカードの埋蔵メモリに異なる。
Kpn	秘密復号鍵	携帯電話機	コンテンツ再生回路(携帯電話機)固有の復号鍵 ※携帯電話機の埋蔵メモリに異なる。
Kmci	秘密復号鍵	メモリカード	メモリカード固有の復号鍵 ※メモリカードの埋蔵メモリに異なる。
Crtn		携帯電話機	コンテンツ再生回路のクラス証明書。認証機能を有する。 (KPpn/Crtn)KPmaの形式で出荷時に記録 ※携帯電話機の埋蔵メモリに異なる。
Cmci	クラス証明書	メモリカード	メモリカードのクラス証明書。認証機能を有する。 (KPmci/Cmci)KPmaの形式で出荷時に記録 ※メモリカードの埋蔵メモリに異なる。

【図5】

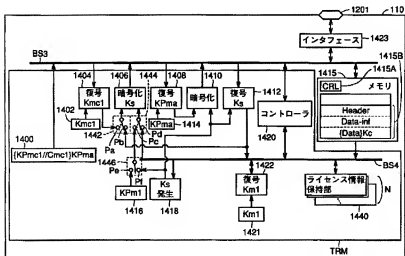




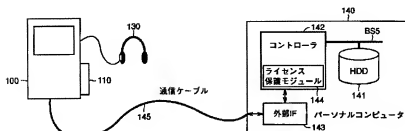
【图6】



【圖 7】



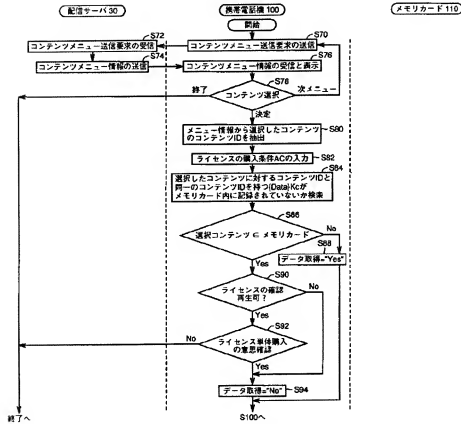
【圖 18】



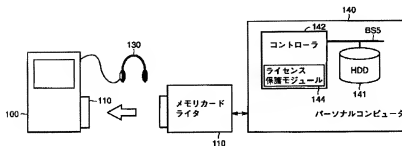
【図 8】



【図9】

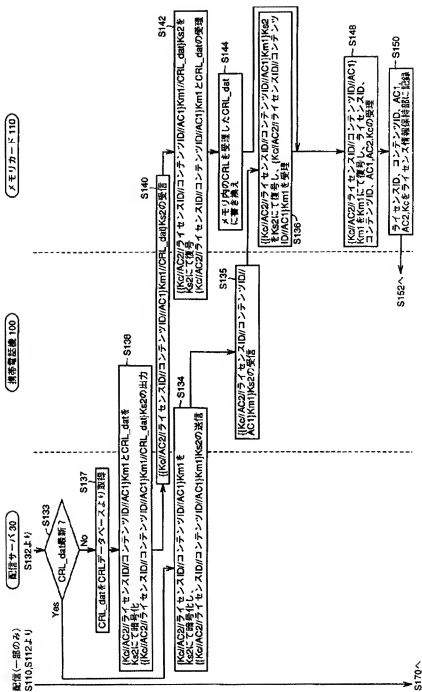


【図19】

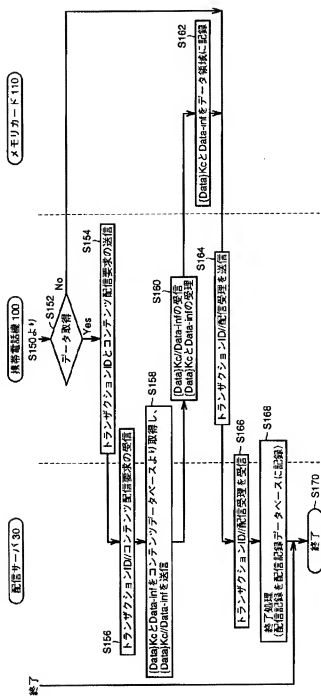




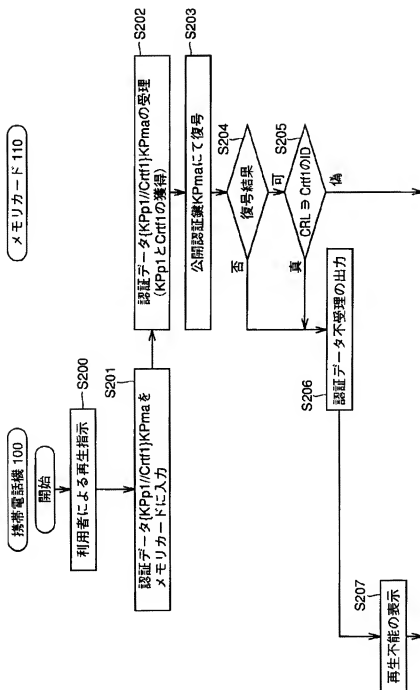
【図11】



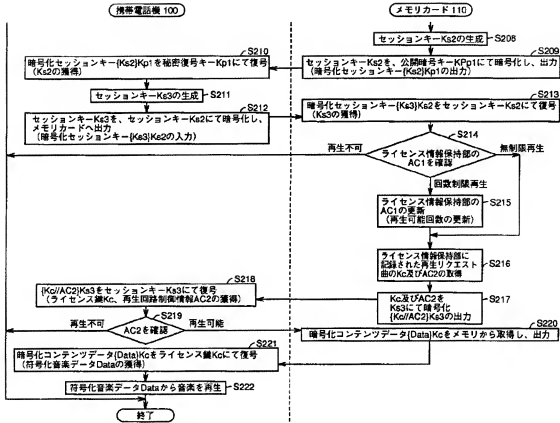
【図12】



【図15】



【図16】





【図17】

